SOMETIMES...
THE ONLY WINNING MOVE IS
NOT TO POST.

MASTODON OPSEC

TL;DR

If you just want a list of best practices to lock down your Mastodon, here they are:

1. **Make your profile with care (it's public)**
2. **Use a unique handle, username, and profile picture**
3. **Hide your social graph**
4. **Disable showing app used to post**
5. **Practice collective security culture**
6. **Be aware of file metadata**
7. **Post carefully**
8. **Lock your account**
    a. **Require follow requests**
    b. **Set default posting privacy to Followers-only**
    c. **Screen your followers**
    d. **Consider opting out of Mastodon's "discoverability" features**
    e. **Opt out of search engine indexing**
    f. **Don't trust your followers**

you will fail. There is no such thing as perfect security. There are always mistakes, bugs, and vulnerabilities you can't account for. But this is the nature of security! It's a constantly evolving war or attrition, not a static state you can research once and thereafter be an expert on. This can contribute to the sense of hopelessness... but really, it means that the more you do, the better, yet every little bit counts.

Finally, consider that sometimes the winning move is not to post :)

Notes and sources:

1. https://distro.f-91w.club/fedizine/
2. https://crimethinc.com/2020/08/26/doxcare-prevention-and-aftercare-for-those-targeted-by-doxxing-and-political-harassment
3. Mat2 is one metadata removal tool: https://0xacab.org/jvoisin/mat2
4. See this article for more contemporary examples: https://www.csrc.link/read/who-wrote-that.html

This guide was written in early 2023 and can be found online at https://distro.f-91w.club/masto-opsec/

For your e-mail too

The e-mail account you used to sign up for Mastodon should also have a *strong and unique* password. If someone breaks into this e-mail, they might be able to request a password reset to get into your Mastodon account.

Use a password manager

Keeping track of many strong and unique passwords can be difficult. Writing them down in a text document on your desktop is not the ideal way! Consider using a password manager like Bitwarden. Most password managers will also have a good password generator, making it easy to come up with strong and unique passwords.

Set up two-factor authentication (2FA)

Mastodon supports 2FA using Google Authenticator-compatible apps that you run on an Android or iOS device. This can really lock down your account, so that your password and access to your mobile device are required to log in.

Pep talk

Reading this might have made you feel like dealing with "operational security" is both overwhelming and hopeless. How can I possibly remember all of these considerations all of the time? Surely the NSA can read whatever I post anyways, so there's no point at all right?

Here is the parting pep talk to help prevent you being stuck in the headlights. You can just tackle these things one manageable step at time. Most of the suggestions here just involve changing settings in Mastodon. And **every little bit counts**. Every small thing you can do to improve your "operational security" makes it less likely your "adversaries" will be able to compromise you.

It's necessary to try and constantly improve your security practices, but if you fall down the rabbithole of security and try to emerge as an Undoxxable Totally Secure Antifa Super Soldier,

Introduction

This article is primarily meant to help users avoid being doxxed or otherwise having a Mastodon account linked to their Real Life Identity. OPSEC is operational (or operations) security, which is basically a military technical term for the process by which you make it harder for your enemy to find out and use information against you. "Loose lips might sink ships". In this case, rather than preventing Soviet spies from learning the locations of your naval convoy... or whatever... we want to prevent trolls from doxxing your personal details based on your Mastodon account.

This article is specifically for Mastodon users, but keep in mind Mastodon is just part of the Fediverse. `Kolektiva.social` is used as an example instance, since the target audience is anarchist Mastodon users and their friends. But this advice is applicable for users on any Mastodon instance. Most of this information is Mastodon-specific, and some of it is applicable across the Fediverse (or even on social media/the internet in general). Before reading this, it can be useful to understand the basics of how the Fediverse works. Check out the *Fedizine*[1] if you want an anarchist-targeted introduction.

This was originally written in early 2023, based on `Mastodon v4.1.0`. Future versions of Mastodon may have different features, or features that are implemented differently. Check where this was originally published to see if it has been updated!

Adversaries and Threat Models

Everyone's security needs are different: people have different goals, will take different risks, and have different enemies. Often when it comes to security questions there is no catch-all answer that applies to all individuals. It always "depends". I will try to avoid using technical terms like adversary and threat model for the rest of the article, but we should quickly go over these concepts, since they are very useful for understanding your own situation and needs, and then applying security advice or best practices appropriately.

Who are your adversaries? For our purposes, these are your enemies: the people or parties who want to link your Mastodon account to other identities to cause you harm. This could be just associating your Mastodon account with other online identities you don't want it to be associated with. Or it could be connecting it to your Real Life Identity so that you can be doxxed or harassed in real life. Or, an adversary could be someone who already knows your Real Life Identity and wants to find your Mastodon account in order to incriminate you or harass you online. Some example adversaries to think about, which may or may not be applicable to you:

- a boss or someone interviewing you for a job
- a troll
- law enforcement
- an abusive ex-partner
- journalists
- estranged family members
- private investigator working for any of the above

Different adversaries will have different capabilities. For example, think about how a powerful government agency may be able to access your ISP's internet access records, compared to a far-right Twitter troll who might only have what's available on the open internet at their disposal.

What is your threat model? Here, your threat model refers to how you consider all the possible ways your adversaries might connect your Mastodon account to other identities to cause you harm, and then come up with all the possible ways you can prevent them. This will be different depending on your personal situation, and what your goals are with your Mastodon account. A user running a counter-info media collective's Mastodon account might want their posts shared and viewed as widely as possible, but will not want anyone to know who is running the account. Meanwhile, another user may want to share some personal art, thoughts and experiences, and be known to and recognized by their friends, but not make it easy for their family or employer to stumble across their account. Both these users have different adversaries and a different threat model in terms of what they can do to protect themselves.

Preferences -> Notifications -> check "Block direct messages from people you don't follow"

You can also disable notifications from people you don't follow or people who don't follow you, which might just be nice for your quality of life.

Mastodon forks and other Fediverse software

Mastodon is just one way to have a presence on the Fediverse. There are actually many other pieces of software that can be used to run an instance, and some of them may be better than others when it comes to security, privacy, and anonymity.

Hometown is a fork of Mastodon that provides a few extra features over regular Mastodon. Hometown adds an additional Local-only per-post privacy control — these posts are only visible to other logged-in users on the same instance. Hometown also has an auto-deletion feature, so that posts older that a user-defined age will be deleted.

GoToSocial is a newer server software that is similar to Mastodon. It is in early development, but one of it's goals is to have better safety and privacy features.

These are just two examples. There are new pieces of the Fediverse popping up all the time!

Securing your Mastodon account

Finally, just a few words on a related topic, which is best practices for securing your actual Mastodon account to prevent someone from breaking into it or taking it over.

Use a strong and unique password

The password for your Mastodon account should be both a *strong* password (long and/or using many different characters) and *unique* (not the same password you use anywhere else).

Forensic linguistics

Forensic linguistics is the process of determining who wrote a particular piece of writing by analyzing the use of language - things like writing style, word choice, phrasing, etc. Basically the idea that you can identify an deanonymize an author by comparing their writing to samples of writing by a known author.[4] It's how the Unabomber was caught and is now a developed technique for trying to identify anonymous authors! This may be applicable especially if you publish writing under a known identity that you do not want connected to your Mastodon account. Cheers to the linguistics analyst trying to determine the author of this particular article right now!

Time

Your Mastodon account is most likely to be active at certain times of day, especially if there is only one author posting from one time zone. Mapping the density of when your posts appear over time may allow someone to guess at what time zone you live in, if you have a full-time or part-time job and what your work schedule is like, or what your sleeping habits are.

Delete old posts

Sure, search engines and scrapers are trying to scrape and index as much of the Fediverse as they can. But they can't get it all. It can always help if you delete older posts when they are no longer needed or relevant. The less information you provide to your adversaries, the better!

Other notes

Block DMs from non-followers

This doesn't really apply to protecting your identity, but if you are someone trying to avoid harassment online in general, it's worth knowing about this feature. You can opt to block Direct posts from non-followers.

Identities

These days, people are likely to have multiple online identities: different accounts on different websites as well as of course their Real Life Identity (by this I mean their legal name and/or other names they use IRL, address, family, etc... the information typically published when someone is doxxed).

It's important to consider how these different identities interact and overlap and how separate (or not) they are. Often, deanonymizing someone online is a matter of connecting one online identity to another until you reach an account that is easily linked to a Real Life Identity. Consider this example:

- A poster has a Mastodon account that they try to keep fairly anonymous. They like to post riot porn and ACAB memes. But this isn't something they want their boss at the Respectable Concrete Milkshake Factory to know about.
- A troll who doesn't like this poster decides to try and uncover their Real Life Identity and doxx them.
- The troll is able to find the poster's Instagram account because the user uses the same handle on Instagram as on Mastodon.
- On the poster's instagram account, there are photos of the poster at work (at the Respectable Concrete Milkshake Factory).
- The troll calls the Respectable Concrete Milkshake Factory on the phone and tricks a co-worker into revealing the poster's real name.
- The troll doxxes the poster.
- The resulting doxx reveals to the conservative management at the Respectable Concrete Milkshake Factory that the poster has been posting a lot of spicy ACAB memes and they are fired. Fuck that job anyways, but I think you get what this example is trying to show!

This guide will provide some best practices for using Mastodon's safety and privacy features to make it harder for someone to link your Mastodon account to other identities. But it's always complicated, especially with how online everyone is these days. Besides just implementing the tips listed below, try to develop

a general understanding of what your different online identities are for, and how they overlap and are linked. Crimethinc has a great and fairly recent guide about how to avoid being doxxed (and also how to react if you are doxxed).[2] Here are some questions from that guide which I think are useful to repeat here:

Ask yourself:

- How separate are each of these accounts/identities?
- What is public? What is private?
- What does public and private mean in the context of each site?
- What can be found by searching your legal name? (Or any other name that you use IRL?)
- Do you use the same username or email for multiple accounts? Do these cross over into distinct spheres of your life? Take a moment to think about the way in which all of these spheres overlap offline.
- Does your job allow you to be open about your politics?
- How public is your activism? Do you speak to reporters? Do you work at an infoshop?
- Do you filter some or all of your social media content from relatives?
- Are there any references to illegal or controversial activities in a given profile?

Understand Mastodon's posting privacy

General

The Internet is a public place. Most online spaces are public to a degree, whether that is a forum, a subreddit, a Discord, etc. Some "private" online spaces might hide posts from public view like an invite-only Discord, or screen new members like a large Signal group chat. But in any group space online, it's safest to assume there might be someone reading who doesn't have your best interests in mind.

Mastodon is part of the Fediverse, which is, for the most part, an open and public social media network. For example, kolektiva.

Extra anonymity

It was already mentioned that instance administrators (of your own instance, and others) can, in theory, access the contents of your posts, even if they are Followers-only or Direct posts. But administrators and moderators of your instance also have access to other information about your account which can affect your ability to remain totally anonymous: mainly, the IP addresses you have accessed your account from, and whatever e-mail address you used to sign up for your account.

Even if you trust the current individual or team running your instance, keep in mind that instances can change hands, new moderators or admins can come on, or certain adversaries with advanced capabilities may be able to hack into or apply legal means to access the server your instance runs on. Besides following the previously mentioned best practices, here are some other measures you can take.

Use a unique, dedicated e-mail address

Sign up for your Mastodon account using an e-mail address that is unique, and isn't based on a username you use for other e-mail addresses or online accounts.

Always use a VPN or Tor

You can use a VPN or Tor to conceal IP addresses associated with you from your instance. Going this route, it is important to ensure you never log into your account without Tor or a VPN protecting your identity.

A VPN is good, but Tor is better. Most Mastodon instances should have no issues with users connecting over Tor, and some instances (like kolektiva.social) might even operate as a .onion service, which is even more secure.

Wingnut mode

Some users may be in a situation where it's absolutely critical that their Mastodon account not be linked to their Real Life Identity. Here is some bonus advice to consider.

Preferences -> Profile -> Appearance -> uncheck “Suggest account to others”

Opt-out of search engine indexing

This will discourage honest search engines from indexing your public posts, which can make it harder to someone searching for keywords on Google to find your profile/posts. This does not prevent less-than-honest or malicious scrapers from indexing your posts, but it won’t hurt.

Preferences -> Other -> check “Opt-out of search engine indexing”

Don’t trust your followers

Even though you’ve put a lot of work into keeping your account private by screening followers, be vigilant and be careful! Any of your followers could be not who they say they are, and may collect screenshots or posts to be used against you. Always consider how many people follow you, who they are, how well you know them all.

- Mastodon has a pretty nice interface for reviewing who follows you (and who you follow). You can see the last time they were active, if you you are mutual followers of each other, etc.

Settings -> “Follows and followers” to view this!

Caveat about a locked account

Remember that Mastodon is not an encrypted secure communication channel, even if you are posting Followers-only to a Locked account. As was mentioned, besides your followers, admins of your instance, or other instances, or anyone with present or future access to the actual server, might be able to view the contents of your posts!

social is an instance with thousands of active users, but is also connected to thousands of other instances. If you are a kolektiva.social user, and you make a Public post, it can end up being read by many different parties, across the Fediverse and across the Internet. One important take-away is that an individual Mastodon instance like kolektiva.social is not a private forum. Just like other social media, Public posts on Mastodon are visible to anyone on the Internet. That could be other users on kolektiva.social, users on other Mastodon instances, or anyone with a web browser who is not even logged into Mastodon.

To get an idea of what parts of your Mastodon account are publicly accessible, you can try loading the public version of your profile. Open a web browser and make sure you are not logged into your instance. Then navigate to the public web version of your profile.

For a kolektiva.social user, this is at `https://kolektiva.social/@username`

Not all Mastodon posts are public though, and Mastodon does offer account-level and post-level privacy controls. Because these controls are different from the limited options available on corporate social media like Twitter or Facebook, many users have trouble understanding how to use them to the desired effect. Let’s look at how posts work on Mastodon with a focus on who can see what.

Posts

Post Privacy Levels

There are four different privacy levels you can assign to new posts, and this will affect who can see them. The official Mastodon documentation provides a great explanation of the different privacy levels:

Level	Public timelines	Permalink	Profile view	Home feeds
Public	Yes	Yes	Yes	Yes
Unlisted	No	Yes	Yes	Yes
Followers-only	No	Logged in on the same site	In-app or logged in	Yes
Direct	No	Logged in and mentioned	In-app or logged in	No

When you compose a new post, you can click on the little globe icon to select the post privacy level for that post. Different apps will have a similar way to set the post privacy for each new post.

What's Public?

Public Posts

Anyone can see these posts, even people without a Mastodon account. Public posts shows up in the Home timelines of your followers, the Local timeline of your instance (for example, kolektiva.social) and potentially the Federated timeline of other instances. Additionally, any other user on the Fediverse can look up your profile and see your Public posts. And, finally, just like with Twitter, even someone just browsing the web can go to your profile and see your Public posts.

Unlisted Posts

Anyone can see these posts, even without a Mastodon account, but they won't appear in the Local timeline of your instance, or in the Federated timelines of other instances. This means while

- A quick note about Follow Requests from "new" accounts. Because of how federation works, if you get a Follow Request from a very new account, or even an account that is just new to your instance (as in, no one else on your instance has ever interacted with it before), it will appear empty with no profile picture and no posts. This is because your instance hasn't yet loaded all the profile information for this user.
- If you want to see the full profile, you need to view it on the user's home instance. To do this on the web interface for Mastodon, you **open the 3 dots menu and select "Open original page"**:

Consider opting out of Mastodon's "discoverability" features

This one might depend on your personal situation. You may want your profile to be easily discovered or stumbled upon by other people — either people who already know you from elsewhere (IRL or online), or just to meet and connect with other like-minded people. If this is your situation, you may weigh your social desires against the risks of being more visible.

If you may have a profile that might invite certain adversaries to troll, stalk, harass, or doxx you because they disagree with your politics, identity, or personhood, you may want it to be harder to discover your profile. Mastodon has limited discoverability features to "promote" accounts. Your account can be suggested to others in a very rudimentary way, and it can be listed in the "Profile Directory" which most instances make public. Here is kolektiva's Profile Directory: `https://kolektiva.social/directory`

It shows the profiles for "Recently Active" or "New Arrivals" on kolektiva.social, or profiles on other instances that kolektiva users have interacted with.

Even if your account isn't easily found with Google or other search engines an adversary is using, they may be able to find you in the Profile Directory, especially if you are using the same or similar handle or profile images you use elsewhere.

Require follow requests

This will make it so that you can screen and manually approve every user who wants to follow you. Some people also call this locking your account. Any Follower-only posts will only be visible to followers you have explicitly approved to follow you. This gives you very tight control over who can see your Follower-only posts.

Preferences -> Profile -> Appearance -> check "Require follow requests"

Note that doing this will not affect the post privacy of any past posts you made. All your past Public posts are still Public. Any future Public posts will also be Public. If you want them to be Follower-only you have to choose that when you compose the post or use your default posting privacy to Followers-only (see below).

Set default posting privacy to Followers-only

Combined with locking your account (above) this will make it so that by default all your new posts are Followers-only. Only your followers will see your new posts (and you have to approve new followers).

Preferences -> Other -> Posting defaults

You can still opt to make an individual new post Public or Unlisted. This can be useful if you want to make a specific post that is boostable and shareable and can be viewed by anyone on the Internet, not just your followers.

Screen your followers

If you have locked your account, you will probably want to carefully screen new followers. How carefully you do this, and what criteria you use will depend on your individual needs. Perhaps you only want people you have met in real life to follow you, or perhaps you just want to weed out malicious accounts that might just try to harass or doxx you. Sometimes an account requesting to follow you can actually be a scraper designed to save and index all your posts.

they are Public and can be Boosted, they aren't automatically served into Federated timelines where any goon browsing might see it and decide to reply-guy you.

So, Unlisted posts are not hidden, they are just less likely to get attention. You may make a post Unlisted because you do not wish to actively solicit replies from randoms, or because you post a lot and as a courtesy don't want to clutter up the Local and Federated Timelines of others.

Search

In general, Mastodon does not have a built-in search feature. You can search for users if you know their username, and search for hashtags. Some instances might have Search installed, allowing users to search through their own posts, posts they have favorited, or perhaps even all public and unlisted posts on the instance. But by default there is no Mastodon-wide search engine.

That being said, Public and Unlisted posts form part of the public content of the Internet, which is regularly indexed by search engines like Google. Google's indexing of Mastodon and the Fediverse is currently far from comprehensive or complete but that might change in the future.

Mastodon-specific Scrapers

Despite not having search, many people have publicly or secretly built Scrapers to specifically crawl Mastodon and save and index every post they find. Some of these are used to try and build a "Mastodon search engine" and some of them may be kept for "private research". It is safe to assume that any Public or Unlisted posts you make might get gobbled up by many of the Scrapers where someone could find it later.

Hashtags

Hashtags are easily searchable if applied to Public posts. They are a way to boost visibility and discoverability of your posts. This can be a good way to spread a message and reach lots of people, but it can also bring unwanted attention from reply-guys

or people who want to specifically target or harass users of certain hashtags!

What's Private?

Followers-only Posts

- Only users who follow you can see these posts, and they have to be logged into their Mastodon account.
- Followers-only posts cannot be boosted.
- **NOTE** if your account is not Locked (set to "Require Follow Requests") then anyone can just follow you and immediately see all your Followers-only posts! If you wish to use Followers-only posts for privacy, you probably want to also Lock your account. See below for how to do that.

Direct Posts

- Only users who are **mentioned** (@user) can see these posts, and they have to be logged into their Mastodon account.
- Some people treat these like confidential messages (commonly called DMs or PMs) but always keep in mind they are not end-to-end encrypted. They are stored as plaintext in the database of your instance, and in theory are accessible to the Admin of your instance (and possibly other instances!). See below!

But what about Admin's reading my DMs?

Your Admin

Mastodon runs on databases. Your home instance (e.g. kolektiva.social) has a huge database that contains every post every user on kolektiva.social has made. This database is stored in plaintext — it is not encrypted! This means that the system administrator of your server, and anyone else with direct access to the server, can (in theory) dig around in the database and look at the contents of *any* posts, including Followers-only posts and Direct posts.

can greatly determine if an adversary will be able to determine your Real Life Identity. This is a potentially huge conversation, but the main point is to weigh the dangers of posting information that could be used to identify you versus your goals of the account (or using social media at all). Always consider how someone could use the contents of your post to figure out your Real Life Identity. Depending on the purpose of your account, you may want to be careful about posting things like:

- photos you have personally taken
- details about your city, neighborhood, or street
- screenshots from your phone or computer (showing details like what's on your desktop, what browser tabs you have open)
- screenshots from chats, or other social media sites (showing things like your username on other sites)
- photos of or details about your job or school
  - weighing in on local drama

These are just some examples of things you can post that could be used to link your Mastodon account to other identities or your Real Life Identity in ways you do not want. But again, this will totally depend on your account and it's purpose.

Locking your account

You may want a Mastodon account where they can post more personally identifying details (photos, selfies, personal details, interacting with friends), but only to other people you trust to some degree, whether it's IRL friends, mufos (mutual followers, people you follow and who follow you back), or just people you have met in real life at least once. How you screen your followers will depend on you, but Mastodon does provide functionality for locking your account and controlling who can see most of your posts.

If you want to go this route, in addition to the general best practices mentioned above, here are some more practices to lock down your Mastodon account in this way.

> Your Mom knows you run the @SecretAntifaSupersoldier@kolektiva.social meme account. She's very proud of you. She can't help herself from commenting on one of your best memes on your birthday "Happy birthday to my meme-lord offspring! Love you!". She has given your date of birth out to any of your followers who can see that reply!

Considering this, you may want to be careful with who knows you run a particular Mastodon account, and make sure those people understand principles of security culture.

All users should also keep this in mind when interacting with other accounts. Think twice when you reply to or tag other accounts. Are you providing more information about the operator of the account than they typically share? Are you making an assumption about how open someone is with their anonymity?

File metadata

Most people are probably familiar with image metadata, or EXIF metadata. Digital photos will often include this metadata that keeps track of when (and sometimes where) a photo was taken, the make and model of the camera, etc. This type of information can used to identify whoever took the photo.

Thankfully, Mastodon automatically strips this data from any photos attached to a post. However, many types of computer files are tagged with metadata that is not easily visible to the user. This can be information like when and where the file was created, with what software, the author's username, etc. Images that are not attached directly to a post but are hosted elsewhere on the internet and linked to can also still contain this metadata. If you are linking to any images or files (PDFs especially) you have posted elsewhere, take care that any metadata has been stripped from the files.[3]

Post carefully

Besides the above points, it is worth thinking about how to post "carefully" in general. Besides all the Mastodon settings and profile preferences at the end of the day what you post and how

(It's possible that your instance, like kolektiva.social, uses disk encryption, meaning the actual drive that the database is stored on is encrypted *at rest* — when the server is powered off. This might prevent someone from, say, seizing the physical server and then just easily looking through the database.)

The other guy's Admin

There's another important caveat here. The Fediverse is made up of many different instances, some based on Mastodon and some based on other software, who all federate with each other. For this whole federation thing to work, instances send copies of posts to each other when it's necessary. The kolektiva.social database doesn't just contain every post by kolektiva.social users, but thousands of posts from users on *other instances*! That's the magic of decentralization at work.

What this means for us though, is that if you make a Followers-only post, that post, by necessity, gets sent to all the other instances that host any of your followers. This is how your post ends up in the Home timelines of your followers. But! This means that a copy of your post also exists in the database of those other instances. The system administrators *of those other instances* could also, in theory, dig around in their database to view your post. The same is true of Direct posts.

Your Profile

Your Mastodon profile deserves some special attention. Everything on your profile is public, visible to anyone, even someone without a Mastodon account. This includes:

- Handle (@user@instance)
- Display name
- Profile picture ("PFP")
- Header image
- Bio text
- Social graph (who you follow and who follows you), unless you disable it
- All your public and unlisted posts and replies
- Profile metadata & the date you joined

- **This is not the metadata we warned you about**... Profile metadata is what you add to your profile, usually it is where people put links to other social media accounts, their pronouns, etc.

You enter your profile metadata on the **edit profile** page.

General best practices

These are a few settings or practices that are applicable to any Mastodon account. Whether you want to follow each of these will depend on your own specific situation and what the purpose of your account is.

Make your profile with care

Remember that everything on your profile (your handle, username, profile pic, header image, bio text, metadata) is publicly viewable by anyone else on Mastodon and anyone with a web browser. So even if you have a private locked-down account, you still need to be conscious of the fact that what's on your profile is public. Do you want your profile picture to be a selfie? Should you link to other projects or accounts that could aid someone in determining your Real Life Identity? This will depend on how you want this identity linked to other identities and accounts you have elsewhere on the Internet. See the next point for specific considerations about your handle, username, and profile pictures.

Consider making your handle, username, and profile picture/header image unique

These three things are part of your public profile, but they deserve particular mention. Don't use the same or similar handle, username, profile picture, or header image that you for other accounts elsewhere on the Internet unless your intention is to explicitly link your account. You may want to do this, for example if you run multiple accounts for the same counter-info project across social media. Maybe you also just want to make it easy for your Twitter followers to find you, but consider that anyone else will have an easy time looking up your past tweets

in addition to your Mastodon posts if they want to figure out who you really are.

Hide your social graph

This means hiding who you follow and who follows you. There are few reasons to have this turned on, the only reason being to make it easier for new users to find interesting accounts to follow. Generally, it will only allow someone to map out networks, and figure out who follows who. For example you may be careful not to post any content that suggests what part of the USA you are based in, but if a majority of your followers are in Phoenix, Arizona, for no other particular reason, an adversary could guess you are based there too.

Preferences -> Profile -> Appearance -> check "Hide your social graph"

Disable showing app used to post

This one is fairly simple. By default, Mastodon displays the app that a user used to compose a toot. This information can be used to profile you (what sort of phone do you have), or identify which user authored a post if multiple users operate the same account, or help link your account to another Mastodon account (by virtue of using the same rare app).

Preferences -> Other -> Uncheck "Disclose application used to send posts"

Security culture: a collective practice

Even if you are very careful to keep your Mastodon account separate from other accounts and/or your Real Life identity, be aware that your friends can accidentally doxx you! If the fact that you run a certain anonymous Mastodon account is just an "open secret" among your friends, one of them may reply to a post or tag you in a post that reveals some of your personally identifying information, or links the account to your personal account. An obvious example of this is tagging someone in a photo. Here's another example: