Where to learn more:

Here's a list of DIY guides, educational resources, manuals, curated recommendations, and more.

Follow them to learn more about what recommendations we give in this guide. Some specific technologies may fall out of favor, but the big ideas remain the same.

These are all either radically-inclined or technically very valuable. <3

- digitaldefensefund.org/ddf-guides
- ssd.eff.org
- securityplanner.consumerreports.org
- github.com/yaelwrites/Big-Ass-Data-Broker-Opt-Out-List
- riseup.net
- github.com/narwhalacademy/zebra-crossing
- @Queersneverdie - TikTok and elsewhere

Digital Security
Virtual Privacy
& LGBT+ TGNC+ NB+ QIA2s+ +

a brief guide of personas,

recommendations,

and followup resources

What this is

The worst threats facing TGNC people today are IRL ones, genocidal in nature, and fueled by the indifference of a state that would rather use us as a rhetorical tool in culture war than provide us with meaningful safety and dignity. The last thing we need are digital security woes emboldening those threats, which, when left unattended, they often do. Although our individual points of view may be different, our oppressions are often the same, and so too are the threats facing us.

There are a ton of digital security guides out there (some favorites are listed on the back of this pamphlet). And although plenty of those stress the importance of "threat modeling" before deciding what steps to take for protection, few offer examples of those models.

That's what this is: a brief guide on some common threat models that may align with your personal experience.

How to use

Scattered below are personas that might fit closely with your particular POV. Each has a brief summary of its particular characteristics, types of threats they face, and some recommended tips & technologies to keep them safe. There is no one-size fits all; chances are you fit more than one of these. Take the recommendations from each that you identify with, and use them as a starting point. Unfortunately there isn't space here to go into specific products or installation or use guides on all the recommendations; instead use this as a way to build a list of specific tools to learn more about. Many of these require definition, and all require further research on your part. That's the nature of these things. But we promise, once you take the time to strengthen your OPSEC, the habit of doing these things gets easier.

Online Activist / Influencer

Similar to the Drag Performer persona, this person has a unique balance between publicity and privacy that they need to handle in order to keep themselves safe while also getting their work done. Raising awareness is just as important as being able to keep private when need be, so for this person, a careful tending of both is key. Compartmentalizing the messaging and activism away from their personal life is a huge step forward. So too is reducing their digital footprint to avoid doxxing.

RECOMMENDATIONS:
Scrubbing public records databases (voter registration records, business registration records) of personal identifying info like addresses, incident response plans, strong account security (passwords, password manager, 2FA), E2EE messaging apps, strong backup game (encrypted drives, cold backups, redundant backups), community rules about what can and cannot be discussed online, careful attention to never posting pics or media with background of hometown, separate accounts or devices for doing online activism, multiple browsers (especially privacy focused ones like Tor or Brave) for sensitive activities, using a service like DeleteMe or following their DIY guide

Closeted

Exactly as the title suggests, this person's transness remains hidden from most people, or, at least the people closest to them in day to day life. This could be because of personal comfort or safety, from schoolmates, family, coworkers, or the general community they're in. Keeping it that way, until they choose to change it, is of utmost importance.

Compartmentalizing their online activities is key. This means keeping stuff related to their transness separate from everything else, not just because it reduces the likelihood of others finding out IRL, but because it limits the chances that it'll eventually lead back to their closeted self online. Finding Secure communications methods with their online friends is also key. It's easy to forget that our security is overlapped with everyone we interact with.

RECOMMENDATIONS:
Multiple browsers (especially private ones for sensitive stuff, like Tor or Firefox), Signal messaging app, code words with trusted community, burner emails (guerillamail, 10minutemail), long specific passcode to cell phone (turn off FaceID if living with others).

Counter Movement Researcher

For this person, running private, quiet, investigations is crucial for their work. It's less about getting a message out to others, and more about spying on opposition to see what's going on. This person is likely teamed up with others to be the one monitoring for chances of doxxing or harassment campaigns. Maybe they're a journalist. Or maybe they're just keeping their ear to the ground about what directions fascist organizing is taking. This person is familiar with 4chan, kiwifarms, some corners of reddit, Telegram, and the like. They want to create believable sock puppet accounts to maintain cover in these hateful spaces.

RECOMMENDATIONS:
Extremely anonymous web browsing separate from regular activities (Tor, designated email addresses for login credentials, separate passwords), randomuser.me, osintframework.com, AI generated portraits for profile pictures, guerillamail for temporary email addresses, hushed app for multiple phone numbers, GrapheneOS burner device, VPN, airgapped data backups of research materials and findings, reduce digital footprint of day-time persona (opt out from data brokers, follow DeleteMe DIY guide)

Teen

It's bizarre and evil that the vast majority of anti-trans legislation this year is aimed at trans youth. That, on top of school mandated spyware installed on devices, apps like Tiktok and Instagram being practically social requirements to stay up-to-date, bullies coming from all directions including politicians... there's a lot to be concerned about. And chances are teens looking at this category should be looking at a few others in this guide to find what's best for them.

RECOMMENDATIONS:
Strong online account security (long unique & random passwords, 2FA), password manager, VPN or Tor browser when searching for medical advice, Signal for messaging friends, turn off AdID on iPhone and Android, rules with friends about sharing info or pictures of each other online, multiple phone numbers or email (Google voice, protonmail) for sensitive accounts, no personal activity on school-issued devices (especially ones with GoGuardian, Gaggle, Bark, or any other student monitoring software installed)

IRL Activist / Protestor

This person is most at risk when going to protests, canvassing at courthouses, rallying support on the street, going to Pride festival marches, etc. Serious investment of time and energy learning about physical self defense is huge, but so too is the consideration towards surveillance of protests, especially by cops. Generally speaking, this person shouldn't put their name in attendance of protests online, and unless they're trying to raise awareness online too (see the persona for Online Activist), they should keep that stuff just for the streets. Remember, Pride was a riot, and an illegal one. We can't limit the possibilities of our protests just to what's polite, respectable, and legal.

RECOMMENDATIONS:
PACE plan (primary alternate contingency emergency), Burner device flashed with GrapheneOS for protests, social rules and team roles for actions, physical self defense, masking in public (COVID safety provides a reason), covering identifiable tattoos, secure messaging fellow activists (BriarProject for mission based work, Signal for general chat), cryptpad/riseup pad for action planning documents, memorizing ally phone number in case of arrest.

Drag Performer

Drag artists have the unique perspective of needing to balance publicity and privacy. Wanting to promote their gigs, while also keeping themselves and the people coming to see them safe, is a difficult challenge, especially as we see the rise in gun violence popping up at drag events. Online harassment is a high likelihood for folks doing drag, and unfortunately, now so too is IRL harassment and violence. Not to mention deranged drag bans in the so-called effort of protecting children. In this case, relying on the security of club venues and public resources is a better idea than trying to defend oneself in the face of an incident.

RECOMMENDATIONS:
Strong account security (2FA, good passwords, password manager), scrub public records (voting registration records, business license records) in case of doxxing, compartmentalization of day life from drag persona (different emails, accounts, associated profiles), regular inquiry into venue safety & security, relying on venue/club promoters to post address information, refraining from posting any information (including pictures-even with seemingly innocent backgrounds-taken at home) about their home.

Movement Organizer / Community Activist

Being at the center of movement organizing is no small task, not just because it's pitching oneself and a community up against the odds of a state that is indifferent to our demise, but because everyone else's security and safety is often reliant on this person's OPSEC. Not to be too scary, but this person definitely requires some top-notch measures to keep themselves and others safe. This person's biggest risks could be law enforcement, doxxing, coordinated IRL hate campaigns, and more.

RECOMMENDATIONS:
Compartmentalization of movement work/personal life (multiple devices, apps, browsers, email accounts, etc), social rules set with community (code words, restrictions about what cannot be shared with others, designated technologies, incident response plans, community space & location security, regular data backups (redundant backups, cold backups, airgapped versions), burner devices, Signal, OnionShare for resource sharing, strong team roles, divesting from Google Docs (cryptpad, riseup pad, local docs), magic-wormhole & OnionShare for filesharing