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 +
+
+

Doxxing
Self
Defense

What's the risk

Doxxing is the intentional exposure of someone's information, usually by some malicious person or group. It's rarely the last harm to occur. For trans folks, it's often a way to leave them vulnerable to anonymous attacks like calling the police on them (Swatting), street harassment, outing them to people in their lives, false accusations... the terrible list goes on. The risk of being doxxed isn't something just trans people face, however, there is a particular fervor that ghoulish sites like KiwiFarms and others whip up in the attempts to ruin trans peoples' lives, with doxxing at the top of the list of available tactics.

Strategy

Once information is out there, it's extremely difficult, near impossible, to get back. The best you can do now is reduce the amount of information that's already out there, monitor the places where doxxing occurs (especially if you are at high risk), and pre-bake some plans for what to do if you become the target of networked harassment. Below is a handful of tactics to find what's out there, ways to reduce it, and some steps you can take now to prepare for the worst.

Voter Registration Records

If you have lived in and been registered to vote in any of these states, your voter registration information is likely public record and published on websites like voterrecords.com :

Alaska, Arkansas, Colorado, Connecticut, Delaware, Wa DC, Florida, Idaho, Louisiana, Michigan, Mississippi, Nevada, New Jersey, North Carolina, Ohio, Oklahoma, Rhode Island, Utah, or Washington

Go to the website listed above to find the records and appeal to have the information taken down. Even if you no longer live at the address that may appear on that site, that information could still be used as a lead to find where you do live now.

Google Dorking for Ur Name

Pretty much every search engine, Google and otherwise, allows for "advanced search operators" that allows you to narrow results in hyper-specific ways. It's super useful for quickly monitoring hate sites like KiwiFarms for any instance of your name, username, your organization, or any kind of information you want to keep an eye on. Here are some examples:

```
site:reddit.com "Martha Graham"

site:kiwifarms.net "Trevor Project"
```

Both examples above will yield only results from the sites listed after "site:" and the exact phrase listed between the following quotes signs.

There are plenty of other types of "dorks" you can use to narrow results. Search for "cheat sheets" for more examples

Find & Delete Old Accounts

It's easy to lose track of all the different accounts you've made over time. With a username checking tool you can find places you may have forgotten about, and discover that information there could lead back to you now. Deleting and deactivating those old accounts is a very good idea, not to mention finding and removing old information about you pre-transition.

Find your old usernames: namechk.com

Note: this may return some false positives. It's worth cross-checking with other tools that do the same.

Opt Out From Data Brokers

Data brokers isn't often an immediate vector of doxxing, but it's a huge contributor to a person's overall data footprint. Opting out from them now is a great thing to do. You can pay for a service like DeleteMe to do it for you, or, go through the trouble of doing it yourself by following DeleteMe's DIY guide or going through the list compiled at:

github.com/yaelwrites/Big-Ass-Data-Broker-Opt-Out-List

PimEyes

PimEyes is a facial recognition image search engine that scours the web. It's evil, scary to use, but pretty damn effective at finding images of yourself that you didn't know existed. Use at your own caution; it can be triggering to see what's out there. But it's certainly something that people use maliciously.

Plan Ahead

Even if you don't put it down in writing, it's a good idea to think ahead about what you will do if you come under target of networked harassment or a doxxing campaign. Keeping an idea of people you can trust to take over your accounts is a hugely beneficial idea. The psychic burden of dealing with that kind of harassment is too much to deal with, so having a friend nearby is key. If instances of harassment start to pile up, keeping a log of them, and the details of them, is a good idea. It's helpful because it will give you a greater idea of perhaps what information they're working off of, but it could reveal patterns about the attackers themselves.

Chaff

Be careful with this one! It's a pretty tricky thing to do, but essentially, the idea is to put out some misleading information about yourself that would get bad-guys to go the wrong way. You have to be careful to create the information anonymously, and do it convincingly in places where hate campaigns are likely to look. It could also potentially confuse people you would otherwise trust, and raise some suspicion. But it's value cannot be overstated; bad guys stop looking as soon as they've found what they're looking for. Making them think they've found it will call them off, or at least frustrate them enough to decide it's no longer worth it when they realize they're lost.