Safety guide for online harassment and doxxing

Action list

Here's a list of actions in this document. **Green - do these now if you can!**

☐	**Risk Assessment** • **Stress** • **Threats that you need help to respond to** • **People trying to access your accounts** • **People degrading your online reputation** • **People spamming your accounts**
☐	**Take care of yourself and each other**
☐	**Make a safety resource list** • **Identify Resource People**
☐	**Take care of your accounts** • **2-Factor / 2-Step Verification** • **Long-ass-and-complicated-Passwords**
☐	**Reduce data collected about you** • **Sign up for Delete Me**
☐	**Developing less connectable digital identities**

- **VPNs**
- **Browser privacy**
- **Turning off data collection**
- **Varying usernames / private information that you use to sign up for accounts**

Risk Assessment: Harassment and doxxing

About Risk Assessment: Risk Assessment is the ideal place to start safety planning. The purpose of risk assessment is to think about what you're facing and align your resources to address the most likely and most impactful of the risks.

There are a lot of ways you can do a risk assessment. If you're a part of a collective, you could gather and talk about risks you've been facing or safety incidents you've experienced and the impacts of these.

This guide is largely designed around a **high risk for harassment and doxxing**.

Doxxing, when your personal information is revealed online in public ways
Incident sharing

A common tactic for harassment online is doxxing. Doxxing is what a person finds your personal information and makes it public. This can look like a person publishing home addresses and personal information about your family members and contact information. This often comes together with individual harassment such as statements published about an individual, misquoting, tagging on social media.

The purpose of all of these tactics is to overwhelm individuals and prevent them from continuing to communicate and be visible online.

Incident response If you are doxxed, refer to this great resource from Crash Override, So you've been doxed: http://www.crashoverridenetwork.com/soyouvebeendoxed.html

Likelihood: High	You are reading this guide because the likelihood for online harassment and doxxing are **high**.
Impacts	What are some likely impacts? ● Stress - to you, to your collective ● Threats to your physical safety that you need help to respond to ● People trying to access your accounts ● People spamming your accounts ● *What are some others?*

Taking care of yourself and each other

Resourcing ourselves: It's a stressful time. You may already have your own practices for grounding yourself. Whether you do or do not, here are some suggestions for questions you can ask yourself to reflect on things you can do to ground yourself in this time.

In addition, **when we are stressed as individuals, our collectives are stressed**. Also below are a few questions that your group can use to discuss how you ground and renew together and how you manage conflicts that arise (and arise more frequently when people are stressed).

Write your answers somewhere that you can look at again in the future to support yourselves!

What are my online wellbeing practices? How do you stay mindful of my body and mind while I am online?
Who are my support people online and offline?
What are my resilience practices? What routines, rituals, or activities help me to stay grounded?
What are our collective practices for grounding and renewing together?
What are our collective practices for engaging in principled conflict with one another?

Make a safety resource list

In case you are facing an incident and feel like you are exceeding your ability to respond on your own, or you just want more help, make a list of resources you can reach to. Some types of support people listed below.

Who are support people for you? Make a list!

Type of People	**Your people (and contact info)**
Trusted people - You can rely on for personal support. Might be friends, advisors, colleagues, family, etc.	
Legal support - You can rely on for legal advice and support	Ex. NLG
Physical safety support - You can rely on for physical safety support - this might mean someone who can be physically near you and offer support that way or people who have a safe place you are able to go to if you feel you need to.	
Health and wellness supports - You can rely on for medical and mental health support	

Take care of your accounts

Risk: Someone tries to log into your account using a username and password that they know or guess of yours

The following is an excerpt from the blog post: **5 Tips for Online Self-Defense**
https://defendourmovements.org/5-tips-for-online-self-defense/

In this section:

- 2-Factor Authentication
- Strong Passwords
- Password Manager

We do a lot online, from personal and private communication, to public calls to action, to sending and receiving money. For some of us, we have been logging into accounts with usernames and passwords for many years now, and it is no longer a very strong way of protecting our accounts. We tend to reuse passwords and usernames (see this list of the most common passwords on Wikipedia), make passwords that are easy to guess or crack with a computer (test password strength here https://password.kaspersky.com/ – *do not enter your actual password*) and data breaches happen, when a services is hacked for password databases (go to https://haveibeenpwned.com/ to see if your accounts have been involved in data breaches).

At this point, we need more than just our favorite username/password combo to take care of our accounts. Here are 3 ways we can take care of access to our accounts.

2-Factor Authentication (2FA)

Passwords can be stolen or taken and the best way to prevent someone from logging into your accounts if they have your password is to use 2-Factor Authentication, sometimes called 2-Step Verification.

- **Use an app for this such as Authy** to receive your verification codes.
- **Do not use text messages** (SMS) for 2-Factor whenever possible. It has become more common for people to intercept 2-Factor codes through "SIM swapping". (Twitter CEO Jack Dorsey's account was hacked this way.)

Backup codes. When you set up 2-Factor Authentication, you often set up a backup method in case you cannot use your first method. For example, if you are unable to get a code from Authy on your phone for any reason, you can enter a one-time backup code or choose to receive a code in another way.

Strong Passwords

- Use passwords that are **long** (20+ characters), **unique** (not re-used), **not made up of common phrases or information** about you (ex. your pet's name, your street name, your favorite color, your favorite family member's name, etc.), includes **varied** characters (upper and lowercase letters, numbers, symbols)
- Consider using **passphrases**; a short phrase or sentence that is significant to you and vary some characters with capital letters, numbers and symbols (for example "you park$d your C@r SIDEways")

Password Manager

- Choose and start using a *password manager* to remember and generate your long, random, unique passwords.
- Keepass is a free and open source password manager you can install and keep on your own computer.
- Lastpass, Dashlane, and 1Password are products that you can access through a browser (convenient if you are using a borrowed device) or through an app that you install on your computer or mobile device. Lastpass offers a free single-user account. 1Password offers a discount to nonprofits.
- See the Defend our Movements resource on Password Managers

Reducing data collected about you

People Finder Sites

Data Broker Sites - Data brokers aggregate information about you that can be purchased or scraped from public data sources. This might be as simple as buying your information from places where you online shop to using public municipal records.

These sites often have a lot of information from lists of addresses where you have lived to people you may be related to and their addresses. These are resources that people use frequently when trying to doxx individuals.

You'll want to remove yourself from these. You can do it one-by-one, or use a service like **Delete Me** to do this for you. This will take some time. It is not an immediate fix, but is worth starting now.

Delete Me - https://abine.com/deleteme

Examples of Data Broker sites:
Pipl.com - https://pipl.com/help/remove/
Familytreenow.com - https://www.familytreenow.com/optout
Spokeo.com - https://www.spokeo.com/Opt-Out

Guides and more information about removing yourself from Data Broker sites:
Crash Override, http://www.crashoverridenetwork.com/preventingdoxing.html
Hack Blossom - https://hackblossom.org/domestic-violence/
Speak Up and Stay Safe Project - https://onlinesafety.feministfrequency.com/en/

Developing less-connectable digital identities

This is a longer term strategy. It may not be something you need to do right now, but is something to start thinking about and implementing when you're out of this high-stress time.

Online Identity

Consider how you show up online.

- Who have you been or are you online? Do you have multiple online persona?
- How do you keep them separate or do you?

Ex. Myself on a dating app, myself on a different dating app, myself on linkedin, a fictitious persona
Ex. be prepared to show as many as you are comfortable sharing

In order to keep your identities less connectable online, which can reduce the ability of people to harass and follow you online, it takes some work.

A shortlist of tactics in order of less to more work:

- Vary your **usernames** on different sites
- Vary the **emails / personal information** you use when signing up for accounts - if you don't have to use your real name, your real birthdate, do you want to?
- Turn **off location** tracking
- Turn **off biometric and facial recognition** tools
- **Browse more privately**
- **Turn off data collection**: examples on Facebook and Google

Using a VPN

So, you want to do opposition research? Want to look at websites and try not to let people know you were looking? Let's do that with a VPN.

What does a VPN do? A Virtual Private Network, or VPN, lets you connect to the internet using a computer that is not your own.

Why does it help with online identity and privacy? Every device that is on the internet - your computer, your tablet, your thermostat, your phone, has an address called an **IP Address**. It's unique to the device.

If you log into your Gmail with your computer, Google knows you logged in from your computer's **IP Address**. If you visit a website from your computer, that website knows you visited from your computer's **IP Address**.

If you'd like the IP Address that sites see you at to be something that is not linked to your device, use a VPN. Services you log into and sites you visit will see you at the **IP Address of your VPN and not your device**.

What are some options?

- ExpressVPN - https://www.expressvpn.com/
- Private Internet Access - https://www.privateinternetaccess.com/
- Brave Browser (https://brave.com/) - has a built in VPN! (free)

Hands-on with Privacy on your Browser

What information does your browser store and why?
Why Chrome and Firefox

Delete browsing history and cookies

- Chrome: https://support.google.com/chrome/answer/95589?co=GENIE.Platform%3DDesktop&hl=en
- Firefox: https://support.mozilla.org/en-US/kb/delete-browsing-search-download-history-firefox

Private Browsing Mode - Only means that the browser doesn't store information

- Chrome: https://support.google.com/chrome/answer/95464?co=GENIE.Platform%3DDesktop&hl=en
- Firefox: https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-history

More about cookies and trackers

- Wall Street Journal 2010 video explainer: https://www.wsj.com/video/how-advertisers-use-internet-cookies-to-track-you/92E525EB-9E4A-4399-817D-8C4E6EF68F93.html
- How-To View Cookies: https://www.wikihow.com/View-Cookies

Try an ad-blocking plugin:

- Privacy Badger: https://www.eff.org/privacybadger
- Disconnect: https://disconnect.me/
- Adblock Plus: https://adblockplus.org/
- Ghostery: https://www.ghostery.com/

Hands-on with Privacy from Google

Google My Account>Data & Personalization: https://myaccount.google.com

Select: Data and Personalization

- See who Who Google Ads thinks I am. Look at “Ad Settings”: https://adssettings.google.com
- To opt-out of targetted ads, turn Ad Personalization to “Off.” This doesn’t mean that you will not see ads or that Google will not collect information. It just will not use that information to show you ads.
- Look at the data Google is storing about your use of Google products: https://myactivity.google.com/myactivity
- Click through and see the data and turn off what you do not want to keep on. You can Delete data by clicking “Delete Activity By”

Hands-on with Privacy from Facebook

Here’s how to find out what you’ve been categorized as, and how to change it:

- Log into Facebook and look at www.facebook.com/ads/preferences.
- What are the “ad preferences” you see here?
- Scroll down and click on the “Your Information” tab and tap on “Your categories.” Here, you’ll see things about you “based on information you’ve provided on Facebook and other activity.”

You can remove an item by clicking the “X” in the top right corner.

To opt-out of targeted ads
To opt out of Facebook showing you targeted ads from other sites, or from seeing Facebook’s ads on other sites, open your Facebook page and click “settings,” and then “ads.”

Then click on the “ads based on my use of websites and apps” setting and press the “choose setting” button and select “off.” Once you turn this feature off, Facebook says you will still see the same number of ads, but they may be less relevant to you. It also won’t stop Facebook (and other companies) from tracking you. It simply means that information won’t be used to show ads targeted to you.