Individual Preventative Measures Against Doxxing and Online Harassment

Targeted online harassment is an endemic problem in academia today. This harassment sometimes takes the form of doxxing, the practice of publishing someone's private information without their consent. This kind of harassment is politically and ideologically motivated, most often from the organized far-right. The most vulnerable people in academia are also those who are most at risk of harassment and doxxing. This includes academic practitioners who are Black, Indigenous, and People of Color (BIPOC), queer, female, or doing work related to race, racism, gender, anti-oppression, Diversity, Equity, and Inclusion (DEI), and related research areas. It includes people who are early career, without tenure or other institutional power, and particularly includes people who are in more than one of these categories.

Targeted online harassment is a political, and therefore collective problem, and demands collective solutions. However, it is also unfortunately incumbent on the at-risk individual to take measures to protect themselves against these attacks, and that is what this guide is about. For our recommended institutional and administrative measures to protect harassed and at-risk people, please see the “institutional measures” part of the LFP anti-harassment toolkit (**libraryfreedom.org/doxxing**).

If you are currently being targeted by an online harassment campaign, please see the “emergency protocols” part of the LFP anti-harassment toolkit.

The intended audience of this guide is individuals (staff, students, faculty) in academic settings who are at risk of being doxxed. The advice and services mentioned here will be from a US-based perspective; however, most of the information is broadly applicable and we have made an effort to make that clear. This guide is also for people who may not be vulnerable to doxxing, but want to support their colleagues who are at risk.

We made this guide after interviewing people who’d been doxxed, their stories are quoted throughout, without attribution and with consent.

The what, why, and how of doxxing and targeted online harassment **2**

What does online harassment and doxxing look like? 2

What methods are used to target someone? 2

Who is responsible for these attacks and why are they doing it? 3

Your threat model **3**

Four focus areas **4**

Level 1: Information security **5**

Update passwords, password managers, and security questions 5

Level 2: Your support system and other people in your life **5**

Identify your support team 6

~ A note about speaking to law enforcement ~ 6

Level 3: Social media, data brokers, and email **7**
Lock social media 7
Removing your personal information from data brokers 8
Set up a Google Alert 9

Level 4: Additional steps for those at high risk **10**
General higher risk preventative actions 10
FOIA and harassment 11
Protect your financial information 11
Protect your phone information 12

The what, why, and how of doxxing and targeted online harassment

> *"I wish that I had been a little bit more cautious about going into a state school in a red state… [I was the] only person of color, only queer person in my program, so I was the easiest possible target."*
>
> *"Be very very cautious if you enter a space and everyone is the same except for you."*

What does online harassment and doxxing look like?

Targeted online harassment may either appear "out of nowhere", or following a public speaking engagement or publication of some kind, especially that which addresses the political topics mentioned earlier in this guide. The targeted person may receive a flood of harassing or even threatening emails, social media messages, or phone calls. These messages may also target official university accounts, administration, or direct supervisors. Sometimes the messages may contain private information (doxxing), and sometimes the harassers may try to access the target's accounts, particularly social media.

What methods are used to target someone?

Targets may have been the victims of someone secretly recording their class lectures or talks, sometimes even with a paid plant in their classroom. Phrases from lectures or publications can be pulled out of context, or questions in a lecture or talk may be used as a setup to produce a response that can be manipulated. The recording or quotes may then be posted to right-wing forums, blogs, and/or social media, and the followers of these accounts then mobilized into action to harassment campaigns. Sometimes these reports can be amplified by higher followers or more mainstream right-wing outlets, such as Breitbart or Fox News.

Who is responsible for these attacks and why are they doing it?

These attacks are politically and ideologically motivated by the far-right, and intended to censor and discredit academic faculty and researchers whose work is antithetical to far-right ideology. Some of these attacks are well-organized and may be funded, and some are more spontaneous and their sources harder to identify.

Some of the outlets whose stories have led to harassment campaigns, or who directly call for harassment campaigns, include:

- Campus Reform (funded by the Leadership Institute)
- The College Fix (funded by Student Free Press Association)
- Professor Watchlist (funded by Turning Point USA)
- Canary Mission (anonymous, focused on Palestinians and their supporters)
- Young America's Foundation (many donors, including the DeVos family)
- Breitbart News Network (funded by Robert Mercer)
- Project Veritas (does not disclose funding, but has been linked to Charles and David Koch)
- Fox News (owned by Murdoch family)
- 4chan (anonymous imageboard)
- Reddit (semi-anonymous messageboard)
- Safe Libraries (One guy on a personal mission to harass librarians who disagree with him politically)

Your threat model

To help determine what steps to take as preventative measures, it's helpful to write up a personal threat model for yourself. You can do this by answering the following questions:

A. What information are you protecting, specifically? What information about you can be connected with other information in what contexts, and what information must be kept secret?

- Personal Information (name, home address, phone number, bank account, personal email, family members, photos, etc.)
- Professional Information (workplace, work phone number, office, projects you've worked on, etc.)
- Political Information (activist/organizing activities or affiliation, comrades, etc.)

B. From whom?

- Independent reactionaries (neo-fascists, TERFs, etc.)?
- Organizations or platforms (like Campus Reform, criticalrace.org, etc.)?
- Well-funded networks of individual harassers, for example Hindutva who harass those who talk about multiculturalism in a South Asian context
- Police, influential politicians, school board members, wealthy stakeholders?
- Abusers or others who have previously targeted or harassed you?

C. What resources do they have available that could be used to access information about you?

- People search websites?
- Social media decoy accounts?
- Funds? How much?
- Technology skills?

D. What is the most likely consequence if they obtain that information? What form of harassment do you anticipate if this specific information were known by these people/groups?
- Online harassment on public social media accounts?
- Calls and/or emails to your workplace, coworkers, or boss?
- Calls, emails, or harassment to your personal accounts or phone?
- Harassment of people you live with, work with, or your family members?
- Someone showing up in person to your workplace or home? Vandalism? Threats?
- Someone calling the police on you or otherwise endangering you physically?

E. How urgent is this threat?
- Just theoretical/hypothetical?
- Something you're nervous about?
- It's an active threat to be concerned about?
- It's already happening? (see emergency protocols section of the toolkit, libraryfreedom.org/doxxing)

Once you have a realistic threat model, you will have developed your priorities around what precautions to take.

Four focus levels

This document is structured around four categories of preventative measures. Each level loosely corresponds to increasing risk levels.

Level 1 (Basic information security) - This involves precautions relating to information security that anyone involved in anti-oppression work, especially those of marginalized identities and communities, should take to protect themselves and their coworkers.

Level 2 (Your support system) - This step is about building your support team and preparing other people in your life about your doxxing threat. This is for people who have higher visibility and/or are engaging in work that has a higher likelihood of being targeted specifically. Also useful for those who have already been doxxed in the past.

Level 3 (Social media, data brokers, and email) - This category involves removing data about yourself from the public internet.

Level 4 (High risk additional steps) - This step is necessary for those who feel they are at particularly high risk of doxxing, who may need to lock down additional accounts, or consider less common scenarios, like a FOIA attack. ***If you are actively being targeted, see our emergency protocols guide at libraryfreedom.org/doxxing.***

Level 1: Information security

Update passwords, password managers, and security questions

Make sure the passwords to your important accounts (like bank accounts, social media, email, work login) are updated with strong, unique, complex passwords. Do not use simple passwords, like names, birthdays, or passwords like “Password1”. Do not reuse passwords. Store your passwords in a password manager like 1Password. Password managers are encrypted vaults which can securely store your logins for every account.

Password managers: These tools can also generate strong passwords for you to use. You need only memorize your master password for logging into the password manager. Password managers can be installed on your computer or phone. This means that no matter where you are, you can access your password manager any time you have access to the internet.

Security questions: Many accounts will also ask for security questions, such as your mother's birthday, your first pet's name, or the city where you met your spouse. These questions are designed to be easy for you to remember in case you forget your password, but this also means they're usually something that is easy to find about you. You can overcome this security vulnerability by giving false answers to the security questions, then storing the false answers in your password manager.

Two-factor authentication (2FA): 2FA is also an important security step. 2FA requires something you know (the password) and something you physically have (e.g. your phone) in order to access the account. Most accounts have an option for this, but you may have to go digging in security settings. The easiest way to set up 2FA is with a cell phone number, but the most secure method is to use a 2FA app, like Authy, Duo, or Google Authenticator, and some password managers (like LastPass and 1password) have authenticator apps built in.

Level 2: Your support system and other people in your life

> *“I wish that I would have known that I was not alone. I felt very alone, isolated, and powerless until I started talking to other people about my experience. I wish I would have known the power of breaking the silence earlier, even if it was just acknowledging what I was experiencing on social media or sending a note out to my colleagues.”*
>
> *“But at this point I had to call my mother who is in her 70s and say, ‘if somebody calls you asking about me, don't talk to them.’ And my mom, of course, was like, ‘What do you mean?’ And I tried to explain to her what doxxing is. So I'm like, ‘if anyone calls you or emails you--I don't care who they say they are--don't tell them anything about me. And if they go so far as to say that something has happened to me or my child, like anything, whatever the tactic is, call [my wife] first. Don't tell strangers anything about me, where to find me, where I work, nothing. Don't share anything.’”*

Identify your support team

One of the most important things you will need is strong emotional support and solidarity. Begin by identifying those people who you can count on, who will be able to help you in case of doxxing and emotional distress. The best people for your support team are those you trust, who will believe you and be ready to act to help you, especially if the situation escalates. They may need to be on call to monitor online attacks, check your email or social media, or other action items listed below. It's best if your support team can coordinate together. Be prepared for the possibility that some people you thought you could count on may not be supportive to you during this time. Focus instead on those who are able to be there for you.

What does support look like?

- Can someone check email, social media, and other accounts for you while the harassment is happening?
- Can someone keep an incident log of the harassment you're receiving, including where it originates if known?
- Can someone who works with you back you up when you need to tell admin, IT, or campus safety what's happening?
- Can someone check on you often during the harassment and make sure you're okay?
- [Extreme cases] Can someone provide you a safe place to stay if the situation escalates or if your home address is shared?

Who you should talk to?:

- Friends and family
    - Explain in simple and clear terms what doxxing is and why you're at risk
    - Emphasize the support you need
    - Share whether or not they are also at risk
    - Who can be part of your support team?
- Work colleagues and bosses
    - Use the institutional guidelines contained in this toolkit (see libraryfreedom.org/doxxing)
    - Can you ask for support, time off, or a reduction in your workload if this happens?
    - Remove or hide information about you, including direct contacts available online
- Bank or credit cards
    - Set up 2fa and account alerts
- Others: landlord, neighbors, lawyer
    - Only if you get doxxed
    - Keep things on a need to know basis

When talking to friends and allies, be specific about what's happening and the support you need

- That you're at risk of being targeted
- How that affects you, and how it can affect them
- What they need to do to minimize the harm
- How they can best support you
- Physical safety needs
- Encourage friends/family to complete some of the anti-doxxing steps. Ex:

    - ★ "Hey here's a thing that might be happening now or soon, bc of my work, pls take these steps to protect me, also be aware that this might be happening to others who work on this, here are things you should be aware of and other groups you should be contacting"
- Points to cover for other scenarios that aren't listed:
    - Saving messages
    - Having someone else read them
    - Messages from supporters with no need to reply

~ A note about speaking to law enforcement ~

> *"But any of the police departments that I have access to… there's four different police departments. And I don't know that any of them has a particularly strong track record with, not just with digital type stuff, but also just honestly anything with queer people, or women-identified, or women-perceived people, or anything like that. So I don't know if I would trust them to actually do that. And also sometimes the response for professors, if there's a threat, is they decide that you're going to have to be removed from campus. Which is ostensibly for your own safety, but also is a punishment, right? It's an admission of your guilt, essentially. That you're somehow complicit in what's happening."*

It's challenging to decide whether or not speaking to law enforcement is right for you in these circumstances. The same things that put us at risk of doxxing and online harassment – race, gender, sexuality, politics, disability status, and so on - are the same things that put us at risk of trusting the police. Some of the people we interviewed for this guide did involve the police, and they met with mixed results from helpfulness to actually making the situation worse. Typically, police were involved when there were threats of violence. Also note that involving campus safety may end up involving local police. Talk to your support team and figure out what's right for you. You're not bad or wrong whatever you decide.

Level 3: Social media, data brokers, and email

> *"[This experience] reminds me to double down and see my social media as an extension of my pedagogy and an extension of my research."*

> *"Now I am much more regimented in checking data brokerage sites… there were lots of little data leaks online that I did not realize, which it is hard to until you experience this."*

Lock social media

Lock down each social media account you have by turning on any of the security settings available and removing all content that could be used to doxx you from your profile or previous posts.

Re-evaluate what information may be leaking by what you do share, especially images (which can capture identifiable places, your face and the faces of people you know), geotags (capturing where and when pictures are taken), and things that may be outside your control, (like your workplace or others who are online posting information relating to you).

- If you use 'linktr.ee,' or another tool, really examine the accounts you link. Seemingly harmless accounts can leak a lot of information (venmo, paypal, et cetera). For example, by adding you as a friend on Venmo, people can find your transaction history and network information.
- Think like a doxxer and their view of the internet--a place where they can find information to harass you and have others target you.
- Go over the security settings in your accounts
    - Social Media
- Consider automatically deleting social media posts after a set amount of time. Bulk delete old tweets with the tool Semiphemeral. You can also plan to delete them on an automatic schedule. See instructions here. There are many customization options, and you can also save a spreadsheet of your old tweets for personal archiving, if you want.
- Delete or hide old Facebook posts in bulk.
- On Twitter, consider proactive blocking of accounts known to be tied to harassment campaigns.
- Considering suspending or deleting your social media / online accounts
    - Account Killer

Removing your personal information from data brokers

> *"I had also earlier googled myself, to see what other identifying information was out there, you know those sites like WhitePages don't just have my stuff, they also have my family's information, including my [young] sister. And where she lives, address, high school, and stuff like that."*

Lots of personal information can get leaked onto the public web via data brokers and data breaches. Unfortunately, name, zip code, and birthdate are enough to locate most people. We want to ensure that this information is not easily discoverable.

Begin by searching for yourself to get a sense of what's out there. As you search, keep a document with the links to the sites where you've found personal information. You'll need those links for the next steps.

What to search for:

- [full legal name] ("Janet Acevedo")
- [full legal name, state/city of residence] ("Janet Acevedo" "New York, NY")
- [full legal name, current institution] ("Janet Acevedo" "CUNY")
- [full legal name, previous workplaces/alma maters] ("Janet Acevedo" "George Hamilton Highschool"]
- [Usernames/Aliases you've used] ("TheJanetPHD7")
    - Keep an eye out for:
        - Legal names, former legal names, aliases

        - City of residence
            - Zip code
        - Photos with identifying information
        - Where you went to school
        - Workplace
        - Place/date of birth
        - Names of relatives
            - Their online security might be weaker than yours; and searching them may reveal more information about you.
        - Email addresses
            - Searching an email address often brings up old accounts with embarrassing or revealing information

When you've created a list of the sites with information about you, search for the name of each site with "opt out", ex. "peoplesearchnow.com opt out." Follow the opt out steps.

We recommend using the Big Ass Data Broker Opt Out List, either by checking each data broker individually to see if they have data about you (more time-consuming, but more thorough) or simply searching for yourself, making a note of which data brokers come up on the first few pages of the search results, and then finding the opt out instructions on the Big Ass Data Broker Opt Out List.

Additional practices for removing data from aggregators/data brokers:

- Make a **new** email to remove data from.
    - **Do not** link this to another email, or a personal phone number (Tutanota or Protonmail). Or you can use a Simple Login alias that you delete after.
- Don't give them any data they don't already have.
- If they ask for an ID, they don't usually check the picture, upload anything.
- If they really dig in their heels, use something that has a photo, name, and nothing else. Like a gym membership card. You can also block out unneeded PII on another form of ID with tape before scanning and uploading.
- Still not working? A passport card may be your best bet. It doesn't have any address information, the PII is harder to dig out, and it's federally issued (US Specific).
- You may have to lie to some places to get your information removed, lean hard on it being a threat to your personal safety. They'll usually come back with it being 'public information that they just collect', but once harm is involved they're more likely to relent.
- You can also pay to have your information removed from data brokers (eg DeleteMe).

Set up a Google Alert

*__Note__- A Google account is needed for this, and the alert will go to the email address that is associated with that account.

- Go to google alerts
    - ★ **Note**- Google alerts use boolean search logic.
- Starting with an alert for is your legal name. Google will prompt you to set up an alert for 'Me on the Web', using the first two names they have associated with your account (usually first and last, unless you have two first names). For example, "Jane Roe."
- Once you click 'create alert', you'll be given the option for 'More Options', this is where you need to assess your threat model. Google gives you the option to receive alerts from 'at most once a week,' to 'as it happens.' They also give you the option to say where you would like to receive alerts from (news, blogs, web, video, et cetera), what region you

would like (the default will be 'Anywhere'), and how many results ('only the best results' vs 'all results').There is also the option to deliver the results to the email associated with your google account, or directly into an RSS feed.
    - ★ **Note** - When you create the alert, google will display the search results as well as what it would send you for an alert.
- There are several things it's best to keep a google alert on for, as well as several ways you should keep a google alert on for a specific name. We'll use the example of 'Jane Anne Roe' to demonstrate.
    - "Jane Roe" "Jane Anne Roe" "Jane * Roe" "Jane" "Roe" (in the same alert)
    - In general, it's a good idea to keep an alert for aliases that are unique to you, and could be traced back to your legal name, as well as something like an email that you most commonly use.

Email

- Send suspect emails straight to spam. Be vigilant about emails that seem even slightly off, seemingly coming from people that you know. If possible, verify them outside of the email (such as through a phone call).
- Give people alternate emails that aren't obvious. Most individuals and workplaces follow similar naming conventions when it comes to email addresses, so it's usually quite easy to 'brute force' into finding the correct email.
    - Can you request an alternate email from IT? Something that is still descriptive, but less obvious. This can be an alias, or something related to your position.
- Be aware of what you send, especially through a work email. If you or the person you are emailing works at a public institution, harassers may request your correspondence through FOIA, and publicly present anything they find without context. If an email seems potentially risky, have the conversation in person.

Level 4: Additional steps for those at high risk

Here are some reasons a person might be higher risk for doxxing and harassment:

- They've been a victim of a harassment campaign in the past
- They have a public profile of some kind (eg they're known professionally, they have a high social media following, they've published something that's getting attention)
- They are BIPOC, LGBTQ, or part of another marginalized group or more than one
- They're in a very conservative area or institution, or are otherwise isolated

General higher risk preventative actions

- Use an alias (as often as you can, online and in anything associated with where you live)
    - You can use the same alias all the time as long as you are careful not to associate it with your real name. Instructions for setting up an alias are here.
    - You may wish to use thispersondoesnotexist for profile pics on alias accounts

- A recommendation: delete personal Facebook, other social media, etc. It will save data for a number of weeks. Even if deleted you can restart the account later if desired. It is much harder to make an account that's not traceable to you nowadays but this should remove the ability of others to tag you in images, statuses, etc.
- A recommendation: depending on the amount of threat and feeling of security in your own home, staying at another address, reaching out to mutual aid groups, family, friends, etc. might be a good move for you.
    - What someone in this level did: They would leave the state for a month when things got really hot.
- If you are registered to vote, people can look up your home address very easily with your name and birthday. Address Confidentiality Programs (ACPs) usually include preventing the sharing of their participants' voter records to keep domestic violence survivors' addresses private. Each state has different laws, requirements, services, and procedures related to its ACP program. To learn more about the ACP program in your area, search for your state's program here: https://victimconnect.org/learn/address-confidentiality
- Consider opening a personal mailbox, like a USPS PO Box or UPS Store box, to route mail to an address that's not your home.
- Higher risk people may face risk of **swatting**:
    - Swatting is a criminal harassment tactic of deceiving an emergency service (via such means as hoaxing an emergency services dispatcher) into sending a police and emergency service response team to another person's address.
    - This is triggered by false reporting of a serious law enforcement emergency, such as a bomb threat, murder, hostage situation, or a false report of a "mental health" emergency, such as reporting that a person is allegedly suicidal or homicidal and may or may not be armed.
    - ***This can be an especially serious threat for BIPOC or disabled individuals.***

FOIA and harassment

Freedom of Information Act (FOIA) requirements and other local public records laws have been used as an online harassment tactic. Because publicly-funded institutions have a FOIA reporting requirements, many harassers will use this to target individuals and gain access to their email or other work materials.

- Know what your own institution's FOIA requirements are
- Do not use work email to discuss personal matters of any kind
- Do not send email to a colleague's work account from your personal account – your personal account and messages could be disclosed in a FOIA response

Protect your financial information

Below are some credit best practices (US specific):

- Pull your credit reports (annualcreditreport.com), and make sure they are correct.
- Freeze your credit with the big three, so no new lines of credit can be opened. This will prevent almost all attempts to steal an identity. There are smaller brokers though, and freezing with these can cause different problems (like a landlord not being able to pull your background check), but you do have the option to freeze with them as well.
    - Experian, TransUnion, and Equifax (Big Three)
    - Innovis, ChexSystems, LexisNexis, MicroBilt Connect, and NCTUNE
- After freezing, attempt to pull your credit again (you should be blocked).

- This will block people from opening new lines of credit in your name, but it's not foolproof. If you want another layer of security, also implement a fraud alert (also free) with the big three.
- ***Why?*** A credit freeze can be often lifted with commonly found PII if you 'forgot your PIN'. A fraud alert in place will force the vendor to verify additional information about the person before lifting a freeze. Usually a phone call, at the verified phone number attached to the fraud alert (as well as potentially other 'approved numbers'?), and then verification of PII. This is an extreme scenario though, and any measure of security with locking down your credit will help exponentially.

Protect your phone information

> *"So it started with emails requesting interviews, statements... And then I got a phone call from a local-ish area code. So I answered, and it was someone who identified themselves just by name only, asking to meet with me in person to talk about the graduate program. Then I got another phone call. I was continuing to get emails requesting comment on this article, and then got another phone call a week or so later. Somebody identified themselves as one of my former students and they named a class that I had taught at some point a year or so earlier. These things just started to accumulate in my mind. Like this is strange. [We] started scouring and cleaning up and finding old CVs that were floating around, like academia.edu or LinkedIn. Anywhere that might have my phone number. And there weren't very many places, so somebody was digging pretty deep. I don't know. I don't know how they got it."*

Another distressing consequence of being doxxed is receiving toxic voicemails, threats and texts that flood your phone service and fill your inbox. Below are some possible mitigations to that issue.

- **Use a call forwarding service**
    - Call forwarding services can help you easily block and ignore unknown numbers. Google Voice and Twilio are two options for call forwarding. Please note that the call forwarding service is still attached to your real number, but it is a good option for ignoring harassing calls.
- **Protect yourself against SIM swapping**
    - SIM swapping, sometimes called a SIM hijacking attack, is a scam involving hijacking of the Subscriber Identity Module (SIM) chip card found inside smartphones which links your phone number and account information to your mobile provider. Bad actors use SIM swapping as a way to intercept one-time security codes from banks and cryptocurrency exchanges. The victims' email accounts are often compromised prior to the SIM change to allow hijackers to intercept communications from cellular providers. This ensures that the victim will not receive notifications of unusual activity with their accounts. Prevention?
        - Don't overshare your mobile number (e.g. pet stores, prize drawings , etc)
        - Add a PIN to lock your SIM (Google "SIM PIN Settings" for directions)
        - Clear personal information from your social media accounts. Hijackers can use this info to trick carriers into authorizing the swap.
- **Port your phone number**
    - Porting your number is the act of transferring your existing cell number to a new wireless carrier or connecting that number to a masked number. The main

reason to consider porting would be to ensure that all voice messages, texted codes, etc continue to reach you instead of the stranger that receives your old number.

- If you are not switching carriers, consider requesting a port freeze and locking your account to your current SIM.
- A step by step guide for porting your phone number can be found here:
  - How to Port a Mobile Number - WikiHow
  - How to Port Freeze

Thank you to the Rose Foundation
for their generous support of our work.