Community Care
AMS LGBTQ+

https://tinyurl.com/AMSqueersafety

July 2025

LGBTQIA+ scholars have always had to be a care-based network for each other - then and now

Rollback of LGBTQIA+ civil rights for all

Suppression of educational materials dealing with LGBTQIA+ and intersectional knowledge

Defunding of LGBTQIA+ resources, healthcare, community spaces on and off campus

Criminalization of many parts of academic life and scholarly personhood

General climate of bullying and intimidation of vulnerable folks in person and online

why community care

A threat model is a list of the most probable threats to your security and privacy endeavors. Since it's impossible to protect yourself against **every** attack(er), you should focus on the **most probable** threats. In computer security, a threat is an event that could undermine your efforts to stay private and secure.

Focusing on the threats that matter to you narrows down your thinking about the protection you need, so you can choose the tools that are right for the job.

Creating Your Threat Model

To identify what could happen to the things you value and determine from whom you need to protect them, you should answer these five questions:

1. What do I want to protect?
2. Who do I want to protect it from?
3. How likely is it that I will need to protect it?
4. How bad are the consequences if I fail?
5. How much trouble am I willing to go through to try to prevent potential consequences?

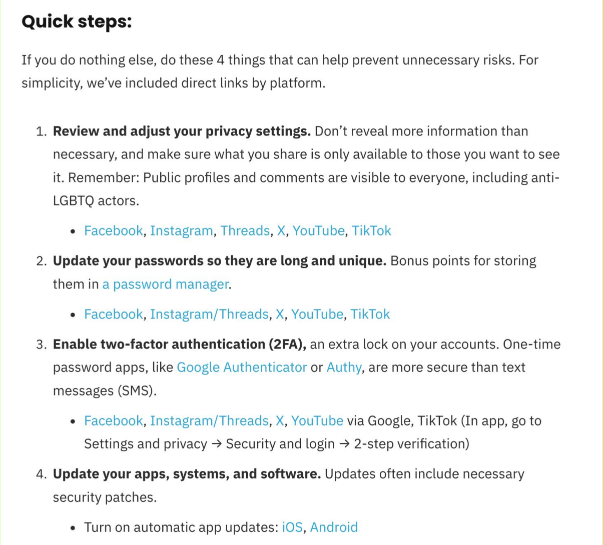
threat models

https://www.privacyguides.org/en/basics/threat-modeling/

GLAAD’s guide to helping LGBTA be more safe online
https://glaad.org/smsi/lgbtq-digital-safety-guide/

Beyond Pride Month: Protecting Digital Identities For LGBTQ+ People

https://www.eff.org/deeplinks/2024/07/beyond-pride-month-protecting-digital-identities-lgbtq-people



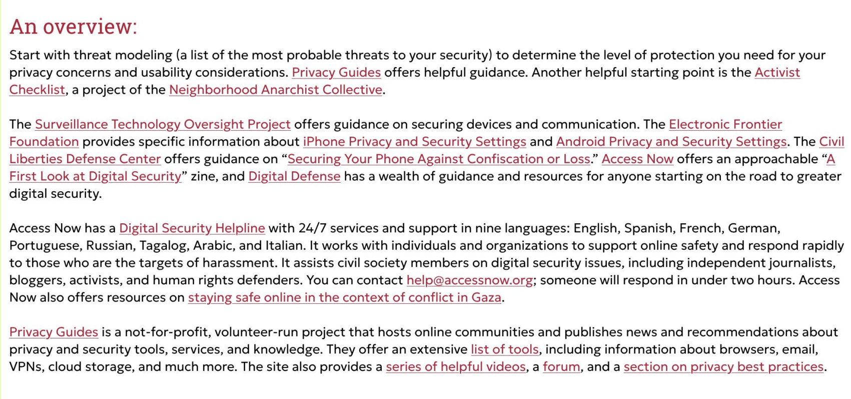
Quick steps:

If you do nothing else, do these 4 things that can help prevent unnecessary risks. For simplicity, we’ve included direct links by platform.

1. **Review and adjust your privacy settings.** Don’t reveal more information than necessary, and make sure what you share is only available to those you want to see it. Remember: Public profiles and comments are visible to everyone, including anti-LGBTQ actors.
   - Facebook, Instagram, Threads, X, YouTube, TikTok
2. **Update your passwords so they are long and unique.** Bonus points for storing them in a password manager.
   - Facebook, Instagram/Threads, X, YouTube, TikTok
3. **Enable two-factor authentication (2FA),** an extra lock on your accounts. One-time password apps, like Google Authenticator or Authy, are more secure than text messages (SMS).
   - Facebook, Instagram/Threads, X, YouTube via Google, TikTok (In app, go to Settings and privacy → Security and login → 2-step verification)
4. **Update your apps, systems, and software.** Updates often include necessary security patches.
   - Turn on automatic app updates: iOS, Android

Personal Digital

American Association of University Professors: Digital Security tips https://www.aaup.org/digital-security-resources



An overview:

Start with threat modeling (a list of the most probable threats to your security) to determine the level of protection you need for your privacy concerns and usability considerations. Privacy Guides offers helpful guidance. Another helpful starting point is the Activist Checklist, a project of the Neighborhood Anarchist Collective.

The Surveillance Technology Oversight Project offers guidance on securing devices and communication. The Electronic Frontier Foundation provides specific information about iPhone Privacy and Security Settings and Android Privacy and Security Settings. The Civil Liberties Defense Center offers guidance on "Securing Your Phone Against Confiscation or Loss." Access Now offers an approachable "A First Look at Digital Security" zine, and Digital Defense has a wealth of guidance and resources for anyone starting on the road to greater digital security.

Access Now has a Digital Security Helpline with 24/7 services and support in nine languages: English, Spanish, French, German, Portuguese, Russian, Tagalog, Arabic, and Italian. It works with individuals and organizations to support online safety and respond rapidly to those who are the targets of harassment. It assists civil society members on digital security issues, including independent journalists, bloggers, activists, and human rights defenders. You can contact help@accessnow.org; someone will respond in under two hours. Access Now also offers resources on staying safe online in the context of conflict in Gaza.

Privacy Guides is a not-for-profit, volunteer-run project that hosts online communities and publishes news and recommendations about privacy and security tools, services, and knowledge. They offer an extensive list of tools, including information about browsers, email, VPNs, cloud storage, and much more. The site also provides a series of helpful videos, a forum, and a section on privacy best practices.

Personal Digital

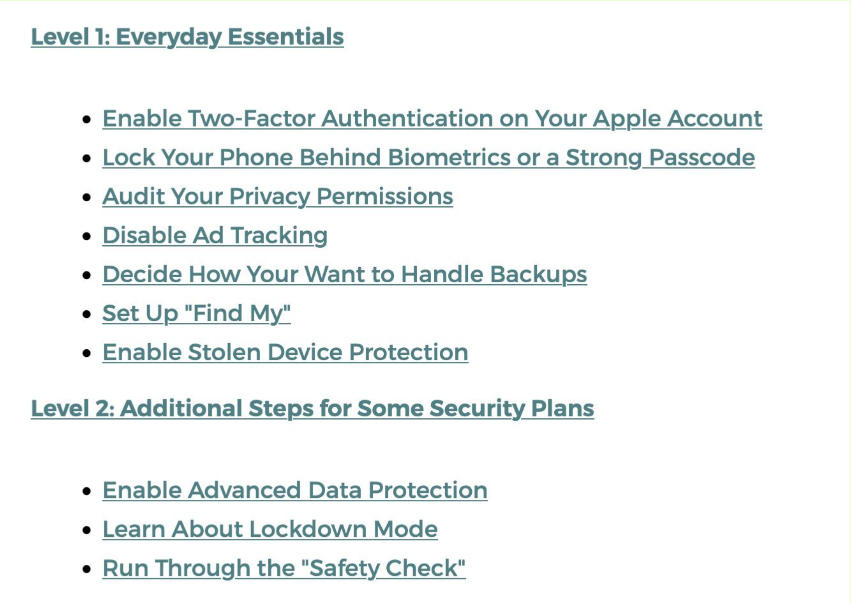
Digital surveillance

Surveillance Technology Oversight Project
https://www.stopspying.org/

iPhone security settings:
https://ssd.eff.org/module/how-to-get-to-know-iphone-privacy-and-security-settings

Android Security Settings
https://ssd.eff.org/module/how-to-get-to-know-android-privacy-and-security-settings

“



Level 1: Everyday Essentials

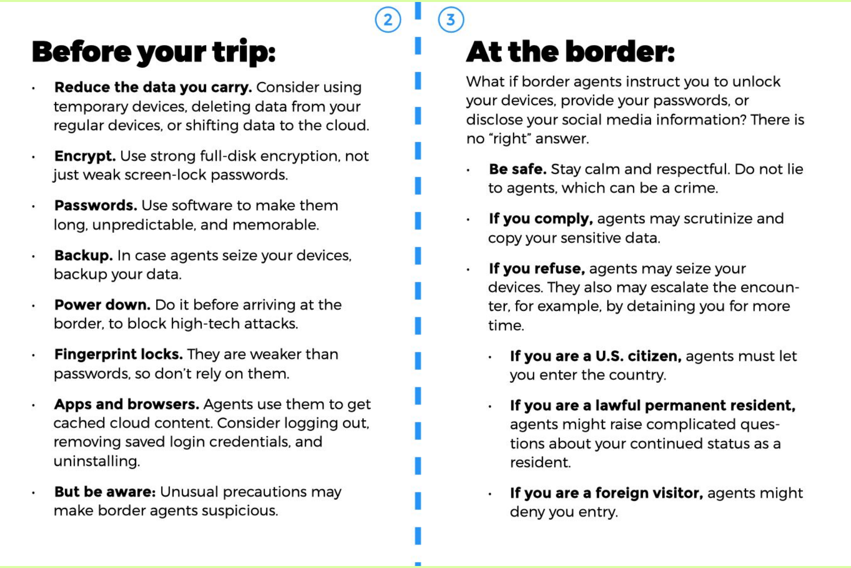
- Enable Two-Factor Authentication on Your Apple Account
- Lock Your Phone Behind Biometrics or a Strong Passcode
- Audit Your Privacy Permissions
- Disable Ad Tracking
- Decide How Your Want to Handle Backups
- Set Up "Find My"
- Enable Stolen Device Protection

Level 2: Additional Steps for Some Security Plans

- Enable Advanced Data Protection
- Learn About Lockdown Mode
- Run Through the "Safety Check"

Personal Safety: borders

Borders: get ready for your crossing



②

Before your trip:

- **Reduce the data you carry.** Consider using temporary devices, deleting data from your regular devices, or shifting data to the cloud.
- **Encrypt.** Use strong full-disk encryption, not just weak screen-lock passwords.
- **Passwords.** Use software to make them long, unpredictable, and memorable.
- **Backup.** In case agents seize your devices, backup your data.
- **Power down.** Do it before arriving at the border, to block high-tech attacks.
- **Fingerprint locks.** They are weaker than passwords, so don't rely on them.
- **Apps and browsers.** Agents use them to get cached cloud content. Consider logging out, removing saved login credentials, and uninstalling.
- **But be aware:** Unusual precautions may make border agents suspicious.

③

At the border:

What if border agents instruct you to unlock your devices, provide your passwords, or disclose your social media information? There is no "right" answer.

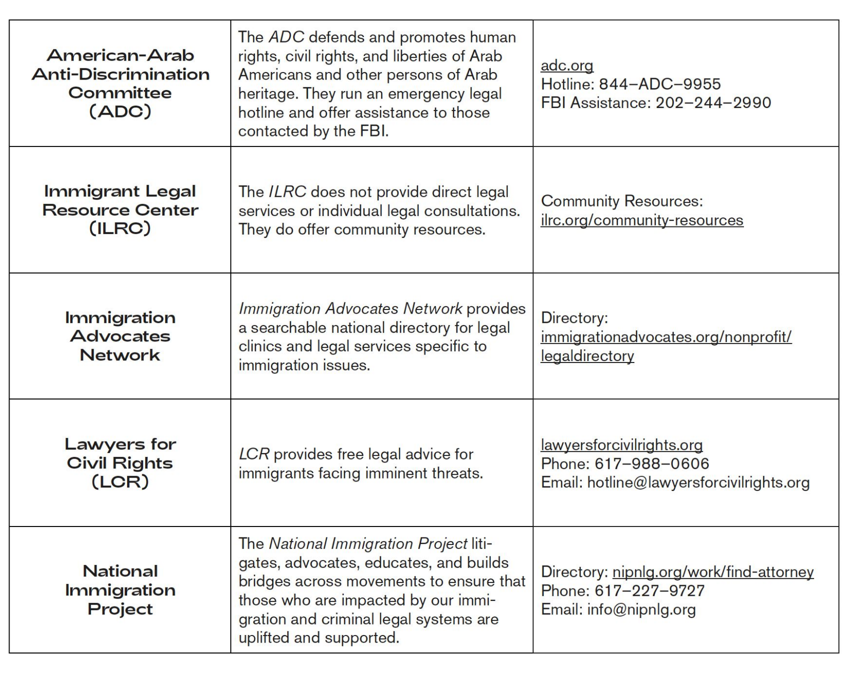
- **Be safe.** Stay calm and respectful. Do not lie to agents, which can be a crime.
- **If you comply,** agents may scrutinize and copy your sensitive data.
- **If you refuse,** agents may seize your devices. They also may escalate the encounter, for example, by detaining you for more time.
  - **If you are a U.S. citizen,** agents must let you enter the country.
  - **If you are a lawful permanent resident,** agents might raise complicated questions about your continued status as a resident.
  - **If you are a foreign visitor,** agents might deny you entry.

International students/faculty - get to know legal services in your city/state as soon as possible.

U.S. citizens - protect your students and faculty - make support plans in advance and have a travel buddy/ tracker.

Legal service clinic locator: https://www.immigrationadvocates.org/nonprofit/legaldirectory/

Lawyers for Civil Rights: PROVIDES FREE LEGAL ADVICE FOR IMMIGRANTS FACING IMMINENT THREATS CALL 617-988-0606 OR EMAILHOTLINE@LAWYERSFORCIVILRIGHTS.ORGMORE



American-Arab Anti-Discrimination Committee (ADC)	The *ADC* defends and promotes human rights, civil rights, and liberties of Arab Americans and other persons of Arab heritage. They run an emergency legal hotline and offer assistance to those contacted by the FBI.	adc.org Hotline: 844–ADC–9955 FBI Assistance: 202–244–2990
Immigrant Legal Resource Center (ILRC)	The *ILRC* does not provide direct legal services or individual legal consultations. They do offer community resources.	Community Resources: ilrc.org/community-resources
Immigration Advocates Network	*Immigration Advocates Network* provides a searchable national directory for legal clinics and legal services specific to immigration issues.	Directory: immigrationadvocates.org/nonprofit/legaldirectory
Lawyers for Civil Rights (LCR)	*LCR* provides free legal advice for immigrants facing imminent threats.	lawyersforcivilrights.org Phone: 617–988–0606 Email: hotline@lawyersforcivilrights.org
National Immigration Project	The *National Immigration Project* litigates, advocates, educates, and builds bridges across movements to ensure that those who are impacted by our immigration and criminal legal systems are uplifted and supported.	Directory: nipnlg.org/work/find-attorney Phone: 617–227–9727 Email: info@nipnlg.org

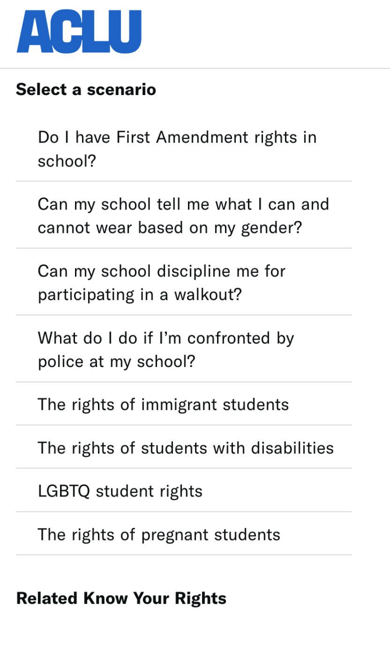
immigration support

Campus free speech

Protest Surveillance Safety https://www.stopspying.org/protest

Know your rights, ACLU: https://www.aclu.org/know-your-rights

Surveillance Technology Oversight Project Protest tips https://www.stopspying.org/protest

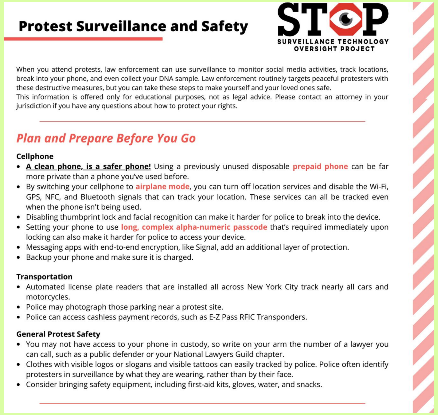


ACLU

Select a scenario

- Do I have First Amendment rights in school?
- Can my school tell me what I can and cannot wear based on my gender?
- Can my school discipline me for participating in a walkout?
- What do I do if I'm confronted by police at my school?
- The rights of immigrant students
- The rights of students with disabilities
- LGBTQ student rights
- The rights of pregnant students

Related Know Your Rights



Protest Surveillance and Safety

STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT

When you attend protests, law enforcement can use surveillance to monitor social media activities, track locations, break into your phone, and even collect your DNA sample. Law enforcement routinely targets peaceful protesters with these destructive measures, but you can take these steps to make yourself and your loved ones safe.
This information is offered only for educational purposes, not as legal advice. Please contact an attorney in your jurisdiction if you have any questions about how to protect your rights.

Plan and Prepare Before You Go

Cellphone

- **A clean phone, is a safer phone!** Using a previously unused disposable **prepaid phone** can be far more private than a phone you've used before.
- By switching your cellphone to **airplane mode**, you can turn off location services and disable the Wi-Fi, GPS, NFC, and Bluetooth signals that can track your location. These services can all be tracked even when the phone isn't being used.
- Disabling thumbprint lock and facial recognition can make it harder for police to break into the device.
- Setting your phone to use **long, complex alpha-numeric passcode** that's required immediately upon locking can also make it harder for police to access your device.
- Messaging apps with end-to-end encryption, like Signal, add an additional layer of protection.
- Backup your phone and make sure it is charged.

Transportation

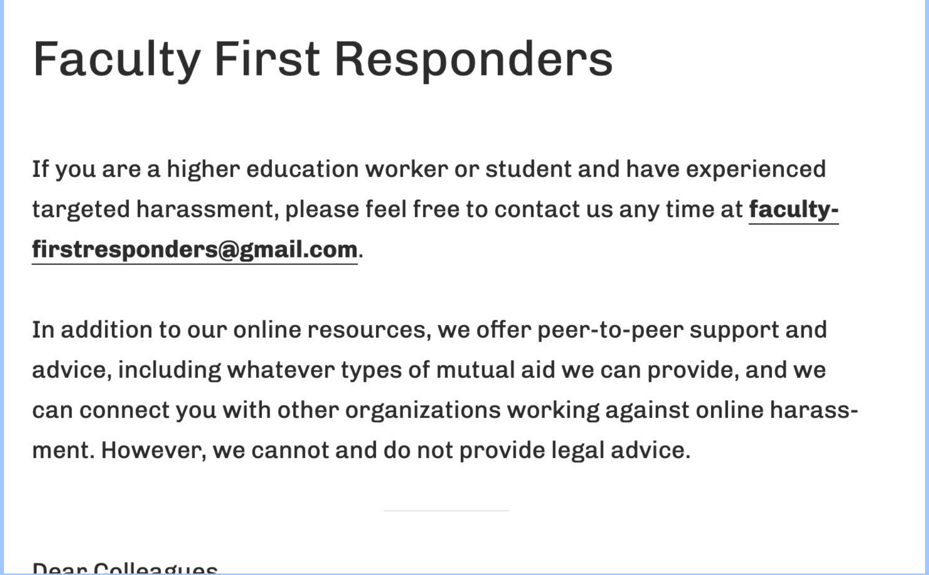
- Automated license plate readers that are installed all across New York City track nearly all cars and motorcycles.
- Police may photograph those parking near a protest site.
- Police can access cashless payment records, such as E-Z Pass RFIC Transponders.

General Protest Safety

- You may not have access to your phone in custody, so write on your arm the number of a lawyer you can call, such as a public defender or your National Lawyers Guild chapter.
- Clothes with visible logos or slogans and visible tattoos can easily tracked by police. Police often identify protesters in surveillance by what they are wearing, rather than by their face.
- Consider bringing safety equipment, including first-aid kits, gloves, water, and snacks.

American Association of University Professors
Academic Freedom Field Guide
https://www.aaup.org/academic-freedom-field-guide

If you are facing a threat to academic freedom on your campus, you can also reach out to the staff at the AAUP's Department of Academic Freedom, Tenure, and Governance (academicfreedom@aaup.org). DAFTG responds to queries from AAUP members and non-members, and provides advice regarding Association-supported principles and standards.



Faculty First Responders

If you are a higher education worker or student and have experienced targeted harassment, please feel free to contact us any time at **faculty-firstresponders@gmail.com**.

In addition to our online resources, we offer peer-to-peer support and advice, including whatever types of mutual aid we can provide, and we can connect you with other organizations working against online harassment. However, we cannot and do not provide legal advice.

Dear Colleagues

academic freedom

"Doxing (or doxxing) is the internet-based practice of researching, documenting, and broadcasting PII (private or personally identifiable information) about an individual or organization to harass and traumatize activists. Additionally, such attacks can also be accompanied by physical violence, intimidation, psychological harassment, weaponized unreality, and disinformation about an individual and/or a movement—all of which have serious implications for our livelihoods and safety."
–Equality Labs, "De-Doxing Guide for Activists"

doxxing

AAUP's anti-doxxing info
https://www.aaup.org/dox-defense-resources

Digital Defense: Doxx Yourself (see what info you have online and how to protect/change it)
https://digitaldefense.noblogs.org/doxx-yourself/

Library Freedom Project: Anti-doxxing zine
https://libraryfreedom.org/resources/

Emergency steps to take if you've been doxxed:
https://onlineviolenceresponsehub.org/doxxing-emergency-steps-to-take

ACLU's doxxing suggestions:
https://www.aclu.org/news/free-speech/some-steps-to-defend-against-online-doxxing-and-harassment

self-defense

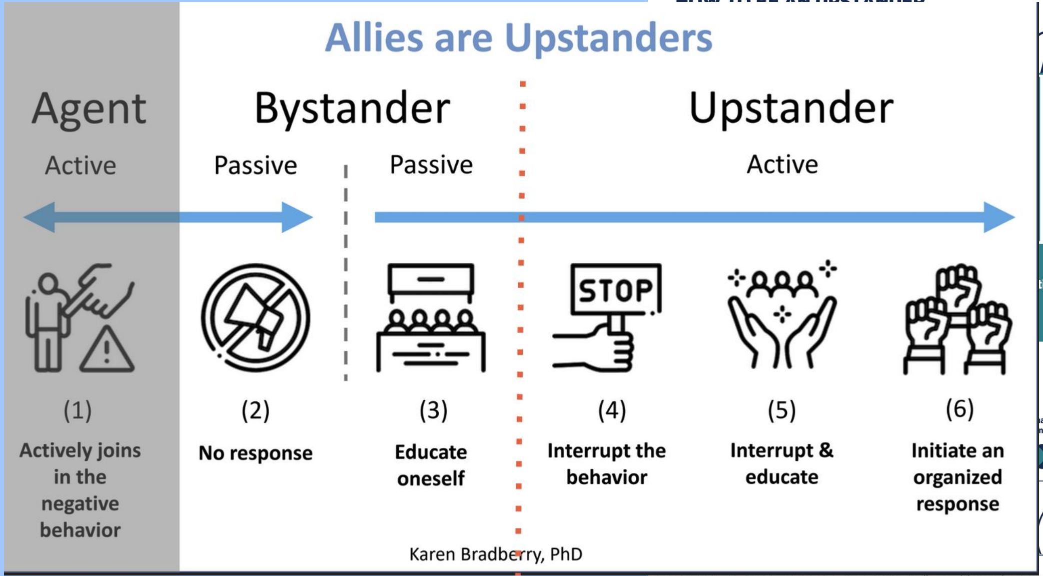
Look for local/regional queer-led self defense classes. If you don't have them, consider helping start one with your local LGBTQIA center/group + a queer martial arts expert

Practice, practice, practice! Self defense techniques work best when they're done so often they become muscle memory. Practice with your friends and attend self defense courses multiple times.

Intro to Self Defense Zine by Soar Over Hate

Self Defense Study Guide for Trans Women (content warning, discusses violence)

Self Defense Starter Kit by Malikah



Allies are Upstanders

(1) Actively joins in the negative behavior

(2) No response

(3) Educate oneself

(4) Interrupt the behavior

(5) Interrupt & educate

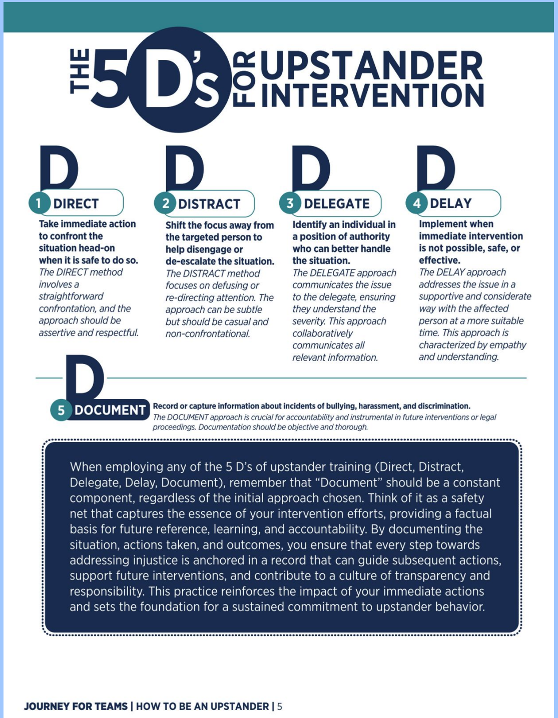
(6) Initiate an organized response

Karen Bradberry, PhD

EDUCATIONAL SHARPENING 5

HOW TO BE AN UPSTANDER

American Psychological Association. *Bystander intervention tip sheet.* Retrieved December 24, 2023 from https://www.apa.org/pi/health-equity/bystander-intervention.
Facing History & Ourselves. *Upstander.* Retrieved December 24, 2023, from www.facinghistory.org/upstander.
Sue, D.W., *et al.* (2021). *Microintervention strategies: What you can do to disarm and dismantle individual and systemic racism and bias.* Hoboken, NJ: Wiley.



THE 5 D's FOR UPSTANDER INTERVENTION

1 DIRECT

Take immediate action to confront the situation head-on when it is safe to do so. *The DIRECT method involves a straightforward confrontation, and the approach should be assertive and respectful.*

2 DISTRACT

Shift the focus away from the targeted person to help disengage or de-escalate the situation. *The DISTRACT method focuses on defusing or re-directing attention. The approach can be subtle but should be casual and non-confrontational.*

3 DELEGATE

Identify an individual in a position of authority who can better handle the situation. *The DELEGATE approach communicates the issue to the delegate, ensuring they understand the severity. This approach collaboratively communicates all relevant information.*

4 DELAY

Implement when immediate intervention is not possible, safe, or effective. *The DELAY approach addresses the issue in a supportive and considerate way with the affected person at a more suitable time. This approach is characterized by empathy and understanding.*

5 DOCUMENT

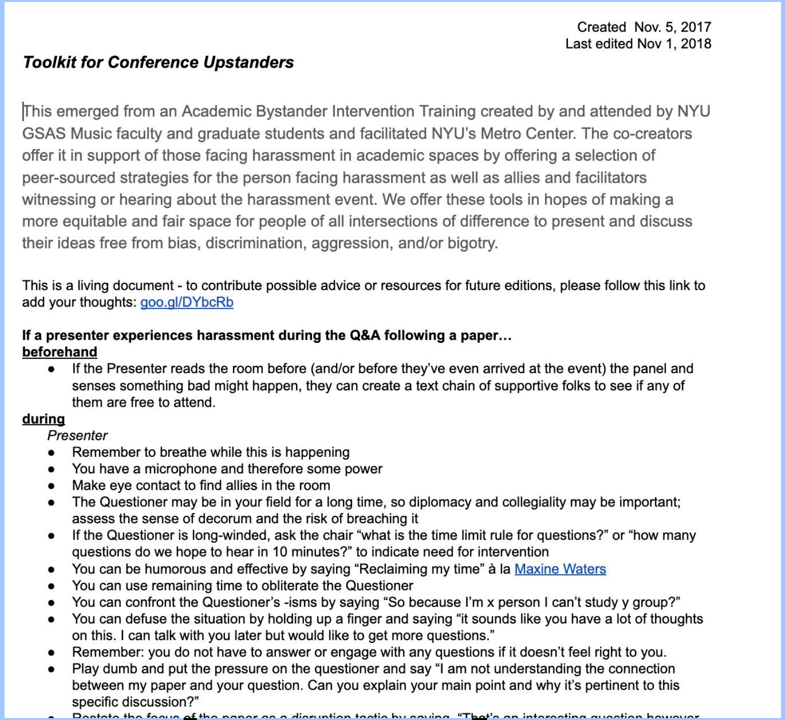
Record or capture information about incidents of bullying, harassment, and discrimination. *The DOCUMENT approach is crucial for accountability and instrumental in future interventions or legal proceedings. Documentation should be objective and thorough.*

When employing any of the 5 D's of upstander training (Direct, Distract, Delegate, Delay, Document), remember that "Document" should be a constant component, regardless of the initial approach chosen. Think of it as a safety net that captures the essence of your intervention efforts, providing a factual basis for future reference, learning, and accountability. By documenting the situation, actions taken, and outcomes, you ensure that every step towards addressing injustice is anchored in a record that can guide subsequent actions, support future interventions, and contribute to a culture of transparency and responsibility. This practice reinforces the impact of your immediate actions and sets the foundation for a sustained commitment to upstander behavior.

JOURNEY FOR TEAMS | HOW TO BE AN UPSTANDER | 5

upstanding

Conference Upstanding



Created Nov. 5, 2017
Last edited Nov 1, 2018

Toolkit for Conference Upstanders

This emerged from an Academic Bystander Intervention Training created by and attended by NYU GSAS Music faculty and graduate students and facilitated NYU's Metro Center. The co-creators offer it in support of those facing harassment in academic spaces by offering a selection of peer-sourced strategies for the person facing harassment as well as allies and facilitators witnessing or hearing about the harassment event. We offer these tools in hopes of making a more equitable and fair space for people of all intersections of difference to present and discuss their ideas free from bias, discrimination, aggression, and/or bigotry.

This is a living document - to contribute possible advice or resources for future editions, please follow this link to add your thoughts: goo.gl/DYbcRb

If a presenter experiences harassment during the Q&A following a paper…
beforehand

- If the Presenter reads the room before (and/or before they've even arrived at the event) the panel and senses something bad might happen, they can create a text chain of supportive folks to see if any of them are free to attend.

during

Presenter

- Remember to breathe while this is happening
- You have a microphone and therefore some power
- Make eye contact to find allies in the room
- The Questioner may be in your field for a long time, so diplomacy and collegiality may be important; assess the sense of decorum and the risk of breaching it
- If the Questioner is long-winded, ask the chair "what is the time limit rule for questions?" or "how many questions do we hope to hear in 10 minutes?" to indicate need for intervention
- You can be humorous and effective by saying "Reclaiming my time" à la Maxine Waters
- You can use remaining time to obliterate the Questioner
- You can confront the Questioner's -isms by saying "So because I'm x person I can't study y group?"
- You can defuse the situation by holding up a finger and saying "it sounds like you have a lot of thoughts on this. I can talk with you later but would like to get more questions."
- Remember: you do not have to answer or engage with any questions if it doesn't feel right to you.
- Play dumb and put the pressure on the questioner and say "I am not understanding the connection between my paper and your question. Can you explain your main point and why it's pertinent to this specific discussion?"
- Restate the focus of the paper as a disruption tactic by saying, "That's an interesting question however

academic upstanding