HARVARD T.H. CHAN
SCHOOL OF PUBLIC HEALTH
Center for Health Communication

Digital safety kit

for public health

About this kit

Online harassment of public health professionals and students is on the rise. Political division during the COVID-19 pandemic has created more risks for people doing health communication and community engagement online.

This kit was created by Sam Mendez for the Harvard T.H. Chan School of Public Health's Center for Health Communication. It is designed to help you prevent and reduce the harm of online harassment in public health.

Read on to learn how to protect each other and call for more institutional support to address this pressing issue.

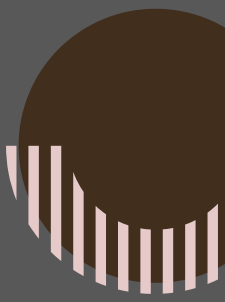
1 Recognize online harassment

2 Respond to online harassment

3 Make a plan to protect yourself

4 What institutions can do

Recognize online harassment



Online harassment can take many forms.

It might resemble in-person bullying via personal insults and threats. It also might take unique forms on social media. For example, harassers can use bots to automate hateful messages and amplify their impact.

The anonymous and decentralized nature of social media can also make it hard to assign responsibility for harassment. Online harassment itself can be traumatic, such as when it involves identity-based hate speech or threats of violence.

Online harassment might also seep into offline spaces. For example, harassers can use social media to coordinate in-person stalking.

What tactics are part of online harassment?

Here are some examples of prominent tactics in online harassment. Learning about these tactics and the terminology around them can help you better understand and describe your experiences:

Astroturfing: coordinated inauthentic online behaviors. Example: a small number of people could use fake profiles to make social media backlash appear as if it is coming from a large crowd.

Concern Trolling: the use of language with a positive tone to mask antagonistic messages. Example: someone might say they support the goals of your public health research, while raising objections in the form of far-fetched hypotheticals.

Cyberbullying: the repeated use of web technologies to demean or harm another person. Example: someone might make public posts to personally insult a health professional.

Cyberstalking: the use of web technologies to repeatedly invade someone's privacy, especially across platforms and communication services. Example: someone might send threatening messages to a public health official across all of their professional and personal social media accounts, as well as their professional and personal email accounts.

Deepfake: a computer-generated image or audio/video clip that provides a false "record" of something that never actually happened. Example: someone might feed footage of real press briefings into software to create a clip purportedly showing a health policy announcement that never happened.

Dogpiling: when a large number of coordinated accounts respond negatively to a social media post or user.

Dog-Whistle: the use of insider language and symbols with hidden meanings. Example: someone might carefully use language to evoke racist stereotypes without breaching a platform's terms of service or facing content moderation.

Doxing: when someone publicly shares another person's private information. For example, someone might publicly share a scientist's home address and cell phone number online.

Hashtag hijacking: the coordinated use of an existing social media hashtag to drown out the intended messaging. For example, a coordinated group might use a vaccination campaign's hashtag to amplify vaccine disinformation and personal attacks against health officials.

Impersonation: posting content online with the aim of deceiving others into thinking it came from someone else. Example: someone might make a social media account to post offensive messages under a doctor's name and photo, with the goal of harming their professional reputation.

Targeting: abusive behaviors that cross a boundary between one's professional and personal life. For example, someone might harass a health professional's child as a means of intimidation.

Swatting: reporting a false crime with the goal of getting a SWAT team to confront someone.

Why is online harassment a concern for public health?

There were at least 1,499 incidents of harassment at local health departments between March 2020 and January 2021. In a 2021 nationally representative survey, 1 in 6 local public health workers felt bullied, threatened, or harassed due to their professional role. This is a serious problem, and we can't expect it to improve any time soon. Surveys show the portion of people in the US who believe it's okay to threaten or harass public health officials increased during the pandemic.

Avoiding harassment isn't as simple as deleting a personal social media accounts. Public health depends on community engagement to work. Event organizers, employers, and publishers regularly share info about public health professionals as part of their jobs. And government funding often requires public availability of public health professionals' contact information.

What public health institutions are at risk?

With political division around public health and the use of social media to coordinate harassment, any institution is at risk. That being said, we know that institutions working toward health equity face heightened risks. Threats of violence can be especially harmful for researchers and practitioners working with Black, trans, and marginalized communities more broadly who have long navigated bigotry and political violence.

Maryland's Frederick County Health Department held an online meeting to discuss the findings of their research into Black maternal health inequities in April 2023. Less than 30 minutes in, racist trolls disrupted the meeting with death threats and graphic imagery.

Boston Children's Hospital became the target of an online disinformation campaign around gender affirming care. This culminated in a flood of harassment, including bomb threats and threats of violence against providers in August 2022. The Children's Hospital of Pittsburgh and Children's National Hospital in Washington, D.C. faced similar harassment campaigns that summer as well.

Who in public health is at risk?

We know that anyone in public health might experience online harassment. However, our public health work takes place in a broader context of racism, transphobia, and other forms of discrimination. Thus we can't assume everyone faces the same kind of risks.

With a lack of data in public health, data from related fields provide important insight. A survey of journalists found that people who identified as LGBTQ+, women, and/or people of color faced higher rates of online harassment than others. A survey of climate scientists found women were more likely to face online threats of violence and attacks on their personal appearance than men. A survey of physicians found women were more likely than men to experience sexual harassment on social media. Such patterns are particularly important for the public health workforce, which is about ¾ women and nearly ½ Black, Indigenous, and people of color.

What public health fields are at risk?

Some areas of public health have long been targets of harassment and disinformation campaigns, e.g. abortion care and stem cell research. Over the past few years, we've seen increased politicization and disinformation around antiracist health research and trans healthcare. However, as the examples below illustrate, anyone in any area of public health is at risk.

Tiffany Dover is a nurse who was working in Chattanooga, TN, when she became a focal point for anti-vaccine propaganda. She fainted upon receiving a COVID-19 vaccine in December 2020. It didn't matter that her fainting was due to a known medical issue, nor that she quickly recovered and went back to work after mere minutes. Conspiracy theorists were convinced that she died. They showed up to her house to demand answers. They called her employer repeatedly. They picked apart her every move on social media for years.

Dr. Peter Hotez is Dean for the National School of Tropical Medicine at Baylor. He became the target of an online pile-on after criticizing a prominent podcast interview with anti-vaccine advocate Robert F. Kennedy Jr. After refusing a debate challenge from the podcast, prominent figures like Elon Musk and Tucker Carlson baselessly attacked his credibility for their audiences. This culminated in harassment at his home in June 2023.

Dr. Angela Rasmussen is a virologist with the Vaccine and Infectious Disease Organization at the University of Saskatchewan. She has described the slow response of Twitter's safety team in the face of very public doxing, physical threats, and sexual harassment. She has noted the toll that prolonged periods of harassment can take on scientists, and the way this tactic can work to drive health experts off social media platforms.

Dr. Akiko Kawasaki is a professor of immunobiology, dermatology, and epidemiology at Yale. She has spoken about the double-edged nature of her growing platform on Twitter. While it has been an effective platform for science communication, it has also been a site of trolling and abusive interactions questioning her expertise. She's also spoken out against bullying, discrimination, and harassment within academia, especially for women of color. She's noted how these different forms of harassment take time away from actually doing her job.

Why is organizational action required?

The problem of online harassment of public health professionals and students is too big to address at just one level. Public health institutions, social media companies, and professional organizations all benefit from the work of public health professionals and students. These institutions also control access to a lot of public health professionals' and students' personal data. Thus they have critical duties to protect us.

Public health and medical institutions can be more proactive in understanding, preventing, and responding to online harassment. For example, the Universities of The Netherlands have adopted policies including supportive measures for scientists experiencing harassment and a data collection platform focused on these incidents. Our institutions also need to listen to the needs of their workforce and rise to meet them.

Social media companies can better prevent harassment on their platforms by listening to creators from marginalized backgrounds. For example, Black streamers and streamers of color petitioned Twitch to make changes in light of rampant automated harassment on the platform.

Lawmakers and government officials can do more to protect the public health workforce. For example, the National Association of County and City Health Officials advocated with the US Attorney General for an increased response to threats of violence against health officials. No single policy will suffice, but they can still support the workforce in meaningful ways. For example, Colorado lawmakers made it illegal to dox public health workers.

Respond to online harassment: An emergency checklist

Online harassment takes many different forms, including: stalking, threats, insults, and hate speech. If you or someone you know is experiencing online harassment, here are some steps you can take to reduce the amount of abusive interactions and cut off pathways for online harassment to spread in person. Remember: it is not your fault if you are experiencing online harassment.

Note that some of these steps assume a supportive work or school environment. It's also important to keep in mind that experiences of harassment may interact with broader structures of discrimination for people of various identities, including women, LGBTQ+ people, Black, Indigenous, and other people of color. These recommendations will be more complicated if the harassment is internal, in which case you may want to reach out to an external advocate, a workers union, or your broader social/professional network.

If you are experiencing harassment

- Assess your priorities and your boundaries. How important is staying visible online? How willing are you to change your online or offline behaviors? What would have to change for you to rethink this?
- Consider changing your social media accounts' visibility settings or deactivating your accounts temporarily.
- Document abusive interactions, including social media posts, direct messages, and emails. Ask a trusted friend or colleague for help if you need to.
- On social media, report content that goes against a platform's terms of service.
- Mute or block harassers on social media as needed. Don't interact with them. Keep in mind that blocking someone is usually visible to them, as they will no longer be able to view and/or interact with your content. In contrast, muting is not usually visible to them, as it prevents you from viewing their content.
- On independent websites, report content that goes against a web host's terms of service. Popular web hosts include GoDaddy and DreamHost. You can search online to find out who hosts a particular website.
- Use social media and search engines to look for any of your contact info that might be circulating online. Report posts and make data deletion requests as necessary. Ask a trusted friend or colleague for help if you need to.
- Check for current log-ins on your social media and email accounts. Log out of any unnecessary devices. Record suspicious log-ins, remotely log them out, and report them, if applicable. Change your password as needed.

If you are experiencing harassment

- Talk to your friends and loved ones about what's going on. This can help you get support and warn them about potential threats.
- Reach out for help from trusted leaders, information technology (IT) specialists, diversity/equity/inclusion (DEI) specialists, and social media specialists at your institution.
- If you are a student, consider invoking a FERPA Block with your school. This prohibits a school from publicly releasing your directory information.

If a colleague is experiencing harassment

- Take online harassment seriously. Personal insults or threats, hate speech, name calling, and leaking of personal information is not the same as a professional critique.
- Do not interact with harassers on social media. Report them. Be careful of blocking harassers or otherwise taking actions that might signal your connections to the person experiencing harassment.
- If you are a close friend or colleague, privately offer to help screen messages, document abusive interactions, and/or audit the availability of personal info online.
- If you are a close friend or colleague, offer to socialize offline.

If my direct report or trainee is experiencing harassment

- Start by asking the person experiencing harassment what they need. Offer any standard supportive measures your employer makes available.
- Advocate for official escalation of harassment reports on social media platforms as necessary. For example, your employer might be able to reach out to the platforms directly.
- Work with your employer to escalate reports to legal authorities as necessary.
- Ensure the person experiencing harassment has the emotional and social support they need within your institution.
- Advocate for the individual's desired level of public support from your employer.
- Advocate for the individual's desired accommodations and assistance from institutional leaders, IT specialists, and communications specialists.
- Work with DEI specialists to better identify and respond to identity-based harassment.
- Help the individual audit the data your employer currently makes public about them. Advocate for data removal as necessary.

Make a plan to protect yourself: A step-by-step guide

You cannot control the actions of harassers. However, there are still steps we can take to make our online spaces safer. Tech companies can work to prevent harassment and bullying on their platforms. Public health institutions can better protect their workforce and their students. You can also take steps as an individual to reduce harm. For example, you can make it more difficult for online harassers to find you in real life. You can also make it harder for them to contact your friends and family.

It's important to know that you have the right to be online and support public health. It's okay if you can't do everything on this checklist. And it's okay if you choose not to. This checklist is about your comfort, boundaries, and what matters most to you.

Step 1: Shield your accounts

It is not your fault if someone hacks one of your social, messenger, or email accounts. But there are still ways you can help protect yourself from low-effort, high-volume attacks and worst-case scenarios.

Make it harder for someone to get into your accounts

- Use a secure password for each account. The longer you make it and the more varied characters you use, the harder it is for someone to guess it.
- Use obscure password recovery questions or fake answers. Data like family names are in public records. Info about pets and jobs might be on social media.
- Use a password manager. Such software can create and store strong passwords for you. Paper logs might be options for accounts you only access at home.
- Change your password regularly. For example, you can set a calendar reminder to change your passwords every 6 months. If someone leaks or steals your password, this makes it less likely it will still work when someone else tries to use it.
- Set up two-factor authentication (2FA) for any accounts you can. This adds a single-use code to your log-in process, which you receive through text message, phone call, email, or a dedicated app. It adds an extra layer of protection in case someone steals your password. Setting up 2FA is available through security or log-in settings on major platforms like Gmail, WhatsApp, Outlook, LinkedIn, and Instagram.
- Create new log-in alerts for any accounts you can. This can help you respond to a hack in real time. For example, Gmail and Instagram can send alerts for log-ins from new locations or devices for your account.

- Use a more secure password for your mobile devices, wherever you can. For example, use a secure password instead of your fingerprint, which can be copied from anything you touch. Use a longer PIN, if your device allows it. Use a password with numbers, letters, and other characters instead of a PIN, if your device allows it.

Limit the damage from one hacked account

- Delete private messages and personal posts regularly. For example, you can set a calendar reminder to delete messages and posts every 6 months.
- Don't put addresses, passwords, and sensitive info in private messages or emails. You can provide such information over the phone or in a messenger application that allows you to delete your messages for everyone. If you have sent such information via email, you can delete it from your account and ask the recipient to delete it from theirs.
- Use unique passwords for each account.
- Use a mix of 2FA and password recovery methods across accounts. If someone gets into one of your accounts with a particular password and 2FA method, they can't just use those exact same steps to access all your other accounts.

Minimize the risk of stolen or hacked devices

- Reduce the number of social media, messenger, and email accounts you keep logged in on your phone, tablet, laptop, etc. Delete as many social media, email, and messaging apps as you can.
- Log out of social media, messenger, and email accounts when you are done with them. Especially on mobile devices.

Step 2: Post like strangers are watching

When you share personal info on social media, you can't know who will eventually see it. You can't know if strangers will use your posts as part of harassment efforts. As such, you can't fully know the risks of sharing information about yourself online. But you can use the reflection questions below to define your own comfort level.

What is your level of comfort with strangers?

- How comfortable are you with strangers knowing where you are in real time?
- How comfortable are you with strangers knowing where you live?
- How comfortable are you with strangers knowing where you work?
- How comfortable are you with strangers knowing about your family?

What are you hoping to gain from sharing information about yourself online?

- Are you sharing your info for professional networking and development?
- Are you sharing your info to receive social support?
- Are you sharing your info for fun?
- Do you want to use less public means to accomplish your goals? For example, you could post a particular question to a workplace listserv rather than on social media.
- Do you want to share less info to accomplish your goals? For example, you could share only your most recent work history on LinkedIn, rather than an exhaustive resume.

Do your posts align with your comfort levels and goals?

- Are you concerned about sharing photo, video, audio, and document metadata? It can include info about files' associated usernames, devices, and time/location of creation. If this does concern you, delete metadata before sharing any media online.
- Are you concerned about an attendee or organizer sharing event guest list information? Event guest lists might be available for attendees, sponsors, or the public. They might include whatever information you shared as part of registration. If this does concern you, check events' data sharing policies. Check if you can opt out of data sharing. You can always register with minimum professional contact info or contact info you create specifically for these kinds of events.
- Are you concerned about your photos, likes, follows, and comments on social media revealing your home or office location? If this does concern you, you can limit your online interactions with local business pages and private neighborhood groups. You can refrain from posting photos/videos taken near where you live, work, or play. You can refrain from sharing information about local news, weather, and other location-specific current events.
- Are you concerned about how long your posts are available for others to look up? If so, you can delete old posts regularly and use more time-limited posting methods (e.g. Stories).

Step 3: Limit your audience

Once something is online, you can't control where it goes. But you can control who you give access to. This can make it easier to track down a leak in the future. It can also lower the number of accounts around you that a harasser might target.

Minimize your known audience to your comfort level.

- Clean up your friends lists and social media connections regularly.
- Customize social media privacy settings so you are comfortable with who can officially view your posts.
- Leave old group chats, Facebook groups, online forums, etc. Try to delete your old messages before you leave.
- Delete your inactive social media accounts.

Delete public data where you can.

- Request data deletion from popular databases like Spokeo and Whitepages.
- Use a subscription service like DeleteMe or Incogni to manage data removal requests from a wide array of data clearinghouses.
- Reach out to old employers and schools if you want them to remove your info from their websites. Your point of contact will be context-specific, e.g. a professor who runs their lab's social media accounts, or a department administrator who shares alumni updates.

Look up your own personal information online. Repeat the above steps if you don't feel comfortable with the level of information you find.

- Search for yourself on multiple search engines, databases, and social media apps.
- Use a reverse image search to find photos of yourself online.
- Set up Google Alerts for the search terms you used to look up your info online.

Step 4: Block off work from other social circles

Consider whether you want all of your social circles to connect to each other. For example, if someone harasses you online at work, you might want to make it harder for them to contact your friends and family. You can take these steps to make it harder for someone else to connect information from different parts of your life.

Separate your work and your personal information online

- Don't use personal contact info to network, register for conferences, join Zoom calls, submit articles to journals, or create professional social media accounts.
- If you don't have work or school contact info, you can create new ones for yourself. You can make an email address and Zoom account only for professional purposes. You can get a free phone number through Google Voice or use a paid VoIP service. You can use a P.O. box or virtual mailbox service. This way, you have contact info you can give out more freely and replace if need be.
- Don't register a professional website with your personal info. Register through your employer or make a website using their existing web resources. If you need to register your own web domain, use a proxy registration service so your info is not publicly available in records of web domain registrations.

- Don’t repost content across accounts you want to separate. For example, if someone sees your anonymous personal account post the same photos right before your work account, they might guess the two are connected.
- Remember: someone might piece together your social circles based on your public interactions on social media. Adjust your activity to your comfort level.
- Consider using a pseudonym for personal or professional social media accounts.

Establish your boundaries with others

- Discuss your concerns of harassment with friends, family, and coworkers.
- Ask friends, family, and coworkers to delete posts with info you wouldn’t want to share about yourself.
- Customize your accounts’ platform-specific settings for comment moderation, private message requests, muting accounts, muting posts with specific words, tagging permissions, etc. This helps you control who can interact with you on a specific platform.

Step 5: Leave behind a smaller digital trail

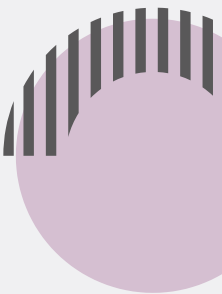
Social media and web technologies play prominent roles in people's social lives and professional development. This can make it harder to leave social media in an emergency. This also means that many people leave behind prominent digital trails that others can follow. You don't have to go off the grid to make it harder for strangers to learn more about you.

Make it harder for someone to get into your accounts

- Download important personal photos and messages from social media. This can help you feel more comfortable deleting posts or whole accounts. This can also make it easier to leave a specific platform in case of an emergency.
- Instead of using social media, share more of your photos and messages 1-on-1 or in small groups via dedicated messenger apps, email, physical copies, etc. This won't necessarily keep that info private. But it can help you leave a less public digital record of your life. This can also make it easier to leave a specific platform in case of an emergency.

Use less public platforms and share less information where appropriate

- Ask yourself what you want from specific communication channels. Ask yourself why you share specific info online.
- Consider whether you can share less info to get what you want. For example, focus on promoting your presentation instead of posting about all the conference events you're attending.
- Consider whether you can use a less public online channel to get what you want. For example, ask for help via a group chat or email list instead of a public post..xt
- Consider whether you can use an offline channel to get what you want. For example, network in-person through trusted colleagues rather than online.
- Consider whether you need to be the one doing the public communication work. For example, work with your employer's communication department to promote your work through media pitches, organizational social media accounts, etc.



What institutions can do

The field of public health relies on visibility and community engagement, including online communication. Unfortunately, online harassment is growing, fueled by political division around public health. Ignoring online harassment can lead to its escalation into real-life harassment and spread to coworkers, family, and friends.

Moreover, online harassment hinders free and open sharing of public health information. This can harm health equity efforts and restrict diversity and inclusion within our field. It can also stall clinical practice and reduce the impact of research.

Public health agencies, universities, and hospitals must actively confront this risk to safeguard our workforce and advance health equity. This proactive approach will look different for each institution. Below, we outline overarching principles and recommend long-term steps your institution can take to foster a safer environment.

Help your workforce and students protect their tech

Technological tools can help protect institutional devices and employee/student professional data. Provide tools and help people understand how to minimize the risk of breached accounts and devices.

- Set up 2FA or physical log-in keys for institutional log-ins.
- Provide phishing protections on institutional email.
- Purchase enterprise accounts for password managers.
- Purchase enterprise accounts for a data removal service. Prominent options include DeleteMe and Incogni.
- Document a device encryption policy. Offer tools for employees and students to encrypt their devices.

Implement web and media policies

Public health institutions can safeguard data in ways that build trust with employees and students. Create policies that center employees' and students' data privacy concerns.

- Create opt-in policies for mentions by name, appearing in photos, and account tagging on institutional social media posts and websites.
- Create opt-in systems for appearing in institutional directories. Give students and employees a choice in the level of detail shared.
- Provide training for online security practices and create a policy around regular training.
- Default to opt-in systems for photographs at in-person events.
- Create a virtual event policy that gives attendees time to change their names, turn off their cameras, or leave altogether before recording starts.
- Ensure contact info from event registrations and meetings are accessible only on a need-to-know basis.
- Make students aware of how to place a FERPA Block to prohibit the release of their directory information.

Implement harassment policies

Emergency response can be more efficient if there are clear resources to draw on. Help employees and students understand the resources available to them in case of harassment.

- Create and share an institutional policy around bullying, discrimination, and online harassment, including how to escalate reports internally and request workplace/classroom accommodations.
- Create templates for public statements, reports to social media platforms, data removal requests, and internal announcements to prepare for future emergencies.
- Create a digital safety team so employees and students know who to turn to in case of online harassment.
- Create an emergency workflow to help people remove information from institutional websites in case of harassment.
- Create and share resources to help document abusive interactions and screen messages in case of harassment.
- Ensure your institution is ready to draw on a crisis communications expert in emergency situations.
- Ensure your institution is ready to draw on legal advice from professionals who understand state-specific laws on harassment and cyberbullying.

Implement social media policies

Social media policies can help promote emergency preparedness. Promote default practices and a professional culture that prioritize safety on social media.

- Provide training for social media and internet conduct on institutional accounts, as well as project- or lab-specific accounts.
- Maintain institutional social media accounts only where you have the resources to manage them in case of emergencies.
- Ensure you have an employee whose job responsibilities include surveying social media to proactively identify relevant disinformation campaigns, especially around areas of work focusing on health equity and marginalized communities.

Engage your workforce and students

Professional development opportunities can help employees and students reduce the amount of personal data they make available online. Support online professional communication and offer offline alternatives.

- Create offline opportunities for professional networking and development.
- Support offline networking and professional development opportunities specifically for people from underrepresented backgrounds in public health.
- Use institutional communication channels to highlight work against racism, ableism, classism, transphobia, homophobia, and other forms of systemic oppression.
- Give all employees and students access to institutional email addresses, phone numbers, and mailing addresses for use in conference registration, journal submission, etc.
- Provide graduating students with an email address to use during a transition period as they leave your institution.

About us

HARVARD T.H. CHAN
SCHOOL OF PUBLIC HEALTH
Center for Health Communication

Harvard Chan School's Center for Health Communication defines, teaches, and shares best practice in health and science communication. We prepare public health leaders of all kinds to effectively communicate critical health information—equipping them to influence policy debates, counter misinformation, and increase the public's trust in health expertise.

Samuel Mendez

Sam (they/them) is in the PhD program in Social and Behavioral Sciences at the Harvard School of Public Health. Their work focuses on organizational health literacy and bridging public health communication research with their background in media studies theory and artistic practice. A member of the Center for Health Communication's Student Advisory Board, Sam led the creation of this kit.

HARVARD T.H. CHAN
SCHOOL OF PUBLIC HEALTH
Center for Health Communication

Digital safety kit

for public health