



FREEDOM OF
THE **PRESS**
FOUNDATION

Bolster Your Digital Safety: An Anti-Hacking, Anti-Doxing Workshop

Tat Bellamy-Walker

Program Manager, Digital Safety Training and Resources, PEN America


Davis Erin Anderson

Senior Digital Security Trainer, Freedom of the Press Foundation


Conversation agreement

- Space for learning and sharing: confidential and respectful.
- Recognize our own and each other's experiences.
- Take space, give space.
- Open and in good faith.
- Self-care: take care to yourselves however you need to.

Our Goal



To empower you with strategies and resources to protect yourself from hacking, doxing, impersonation, & other abusive tactics.



Our Roadmap

1

What is Online Abuse?

- Terminology
- Tactics
- Impact

2

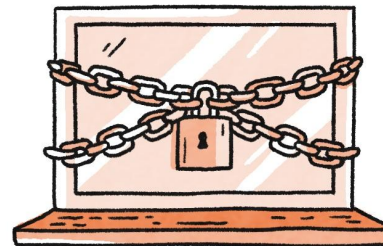
Three vectors of personal information

- Social media
- Public information
- Data brokers

3

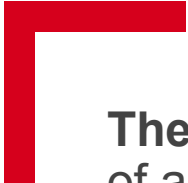
Response tips

- Mute, block, report
- Where to go for help




Online abuse, defined

(aka: cyber harassment, cyber abuse, and online harassment)



The repeated or severe targeting
of an individual or group in an online
setting through harmful behaviors



Online abuse

Tactics

Hateful Speech

Speech (slurs, insults, images, etc.) that targets identity: race, ethnicity, gender, religion, sexual orientation, disability.

Threats

Threats of physical and/or sexual violence intended to instill fear and intimidate target.

Cybermobs

Coordinated attack by group of abusers intended to overwhelm through a barrage of threats, slurs, insults, and other tactics.

Non-consensual intimate images

Distribution of private or manufactured sexually explicit images or videos of target without consent

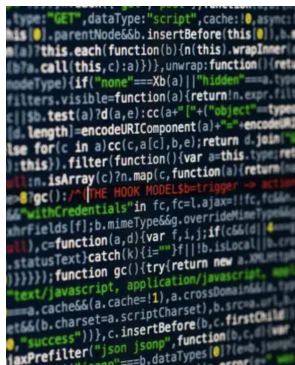


Online abuse

Tactics

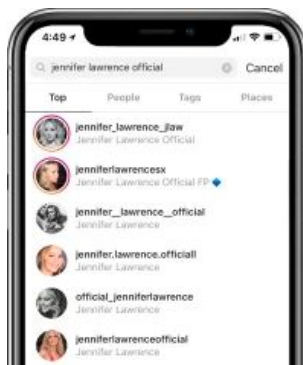
Hacking

The unauthorized intrusion into a device or network, often to steal/leak data, surveil, violate privacy, impersonate, or infect devices with viruses.



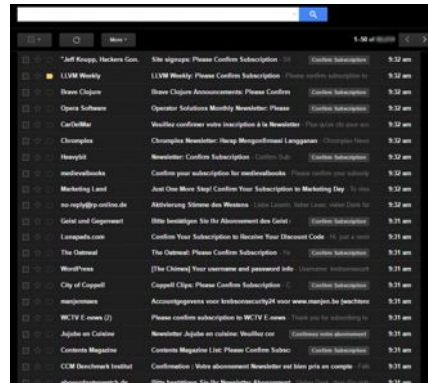
Impersonation

Creation of hoax accounts, usually to post offensive and/or inflammatory statements in target's name to discredit or defame



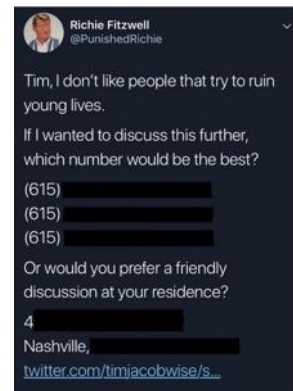
Message Bombing

Flooding target's phone or email accounts with messages meant to disrupt use or block access



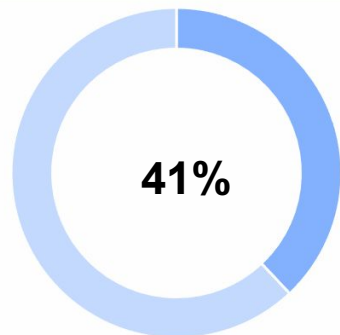
Doxing

Publishing sensitive personal information online to instigate abuse, intimidate, extort, stalk, or steal identity.



Online abuse

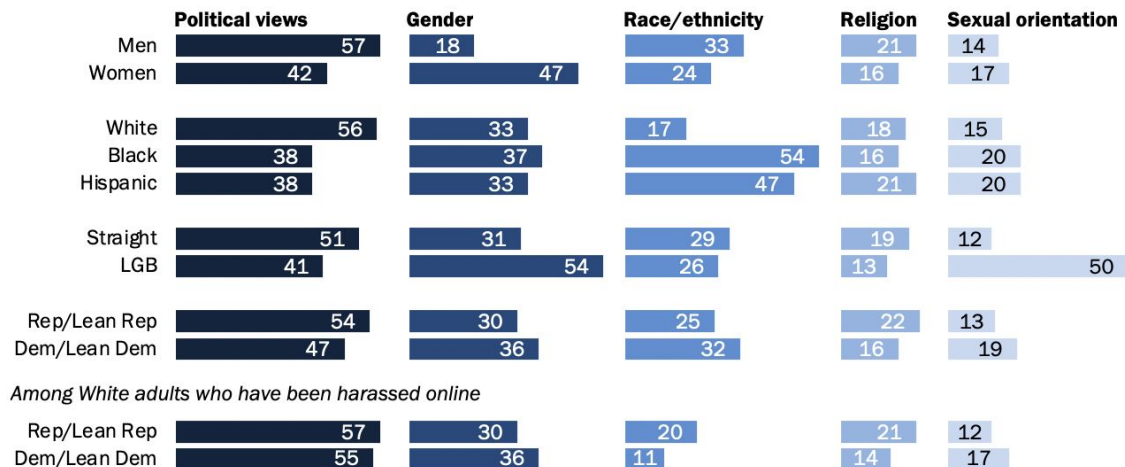
Scope: Demographics of abuse



41% of U.S. adults have experienced online harassment

Black, Hispanic targets of online harassment more likely than their White counterparts to say they've been harassed online because of their race, ethnicity

Among the 41% of U.S. adults who have personally experienced online harassment, % who say they think their online harassment was a result of their ...



Online abuse

Scope: Demographics of abuse

61%

61% of education reporters have been threatened or harassed by their audiences/sources

How, if at all, have you been verbally or physically threatened or harassed by audiences or sources of your education journalism? Please select all that apply.

I have never been threatened or harassed by audiences or sources of my education journalism

39%

Via professional email

37%

Via Twitter

34%

Vectors of online harassment

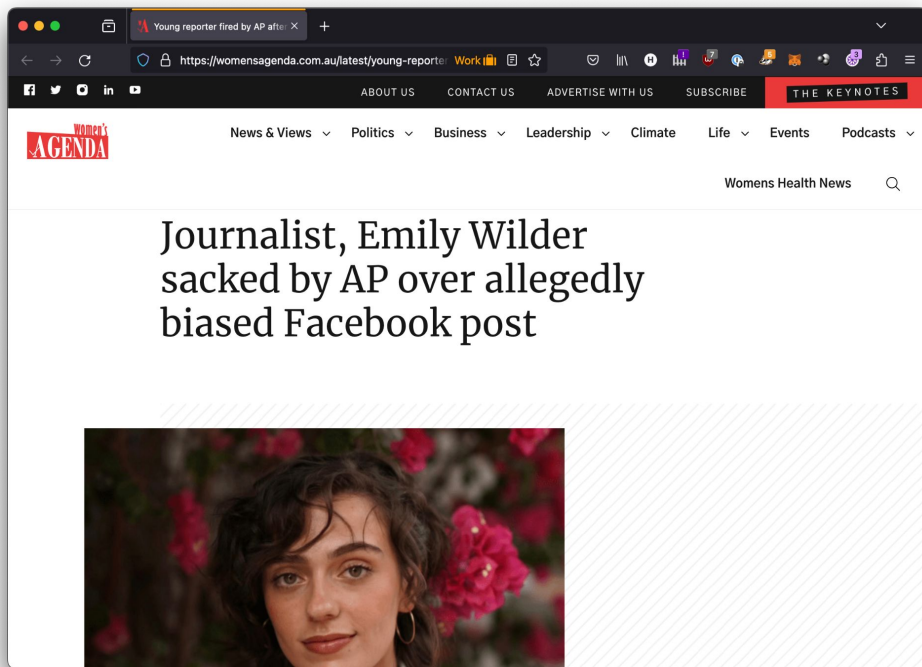
Vector 1: Social Media

Social media

What's at stake?

Your past tweets may be dug up, used as “kompromat” and cause reputational damage, or worse.

“The Stanford College Republicans shared a post Wilder made on Facebook when she was a university student where she described Israel supporter and late US billionaire Sheldon Adelson as a “naked mole rat-looking billionaire”



Social media

Audit your accounts

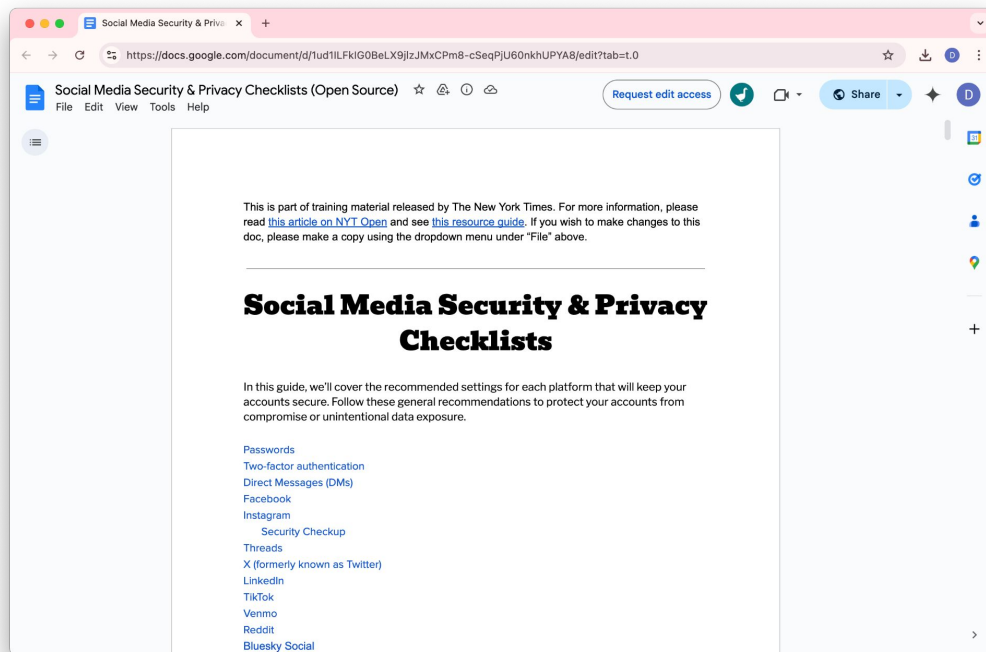
- Go through your posts, and delete any mention of personal information
- Review and adjust your account's privacy settings
- Apply advanced privacy settings around high-risk moments



Social media

Audit your accounts

NYTimes Open has a great resource with step-by-step instructions for popular social media channels





bit.ly/socialmedialockdown

What would you advise?

Raise your hand and share!

Your friend Rose posted this.
What advice would you give?



Social media

Preventing account takeovers

Set strong passwords

Make 'em unique, long and hard to guess

Get a password manager

We love 1Password and Bitwarden

Set tricky security Qs

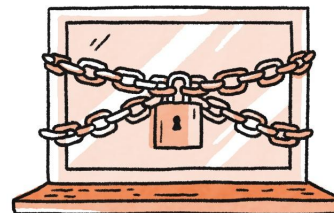
Make up answers & store them in your password mgr

Enable 2FA

Use Google authenticator & Yubico security keys

Set a PIN with your telco

Prevent SIM Jacking by adding a verification code



Separating work from personal

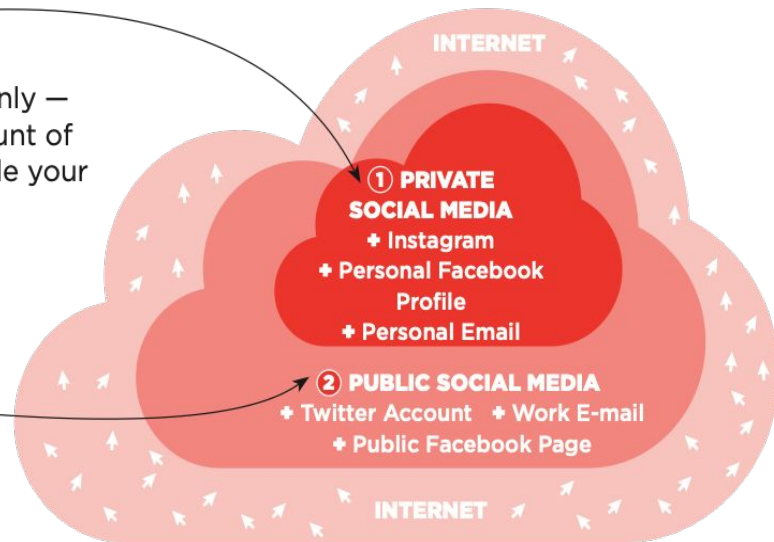
Keep separate accounts

1 Keep your private life, private.

Make sure your personal social media profiles are for friends and family only — not the world. Lock your Instagram account. We want to reduce the amount of personal information that is publicly available. This information can include your home address, mobile number, and identities of family members.

2 ... But keep your public life, public.

Do not lock your Twitter account or deactivate your public Facebook page (not to be confused with your personal Facebook profile!). Your public-facing social media accounts and work e-mail are there to “shield” your private social media.



Keep separate phone numbers

The more widely your phone number is known, the more risk to you

- If someone has your number, they can find you on any platform that's phone number-based or syncs contacts
- If someone has your number they can harass you either themselves or via third parties or dox you

Keep separate phone numbers

Lower risk by giving sources and commercial services a secondary phone number you can access:

- Secondary phone with a secondary number
- Secondary SIM or eSIM in your current phone
- In the U.S., Google Voice phone numbers are free

Get a Virtual Phone Number

- ❑ OPTION 1: Get Google Voice (use your personal gmail to sign up!)
OR
- ❑ OPTION 2: Call your cell phone provider & get a second phone number
OR
- ❑ OPTION 3: Get a second SIM card OR a second physical phone



Vector 2: Public Information

Sources of Public Information

Media

*Newspapers, magazines,
radio, and television*

Internet publications

*Blogs, discussion groups,
user-generated content*

Government records

*Telephone directories,
government websites*

Academic publications

*Journals, conferences,
academic papers*

Grey literature

*White papers, reports,
patents, et cetera*

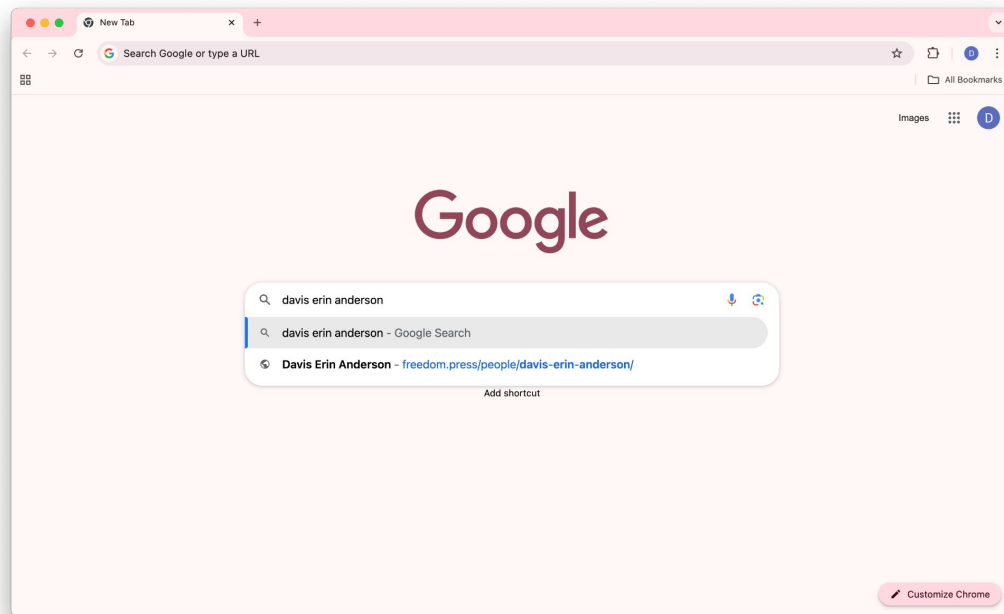


“Doxxing” Yourself



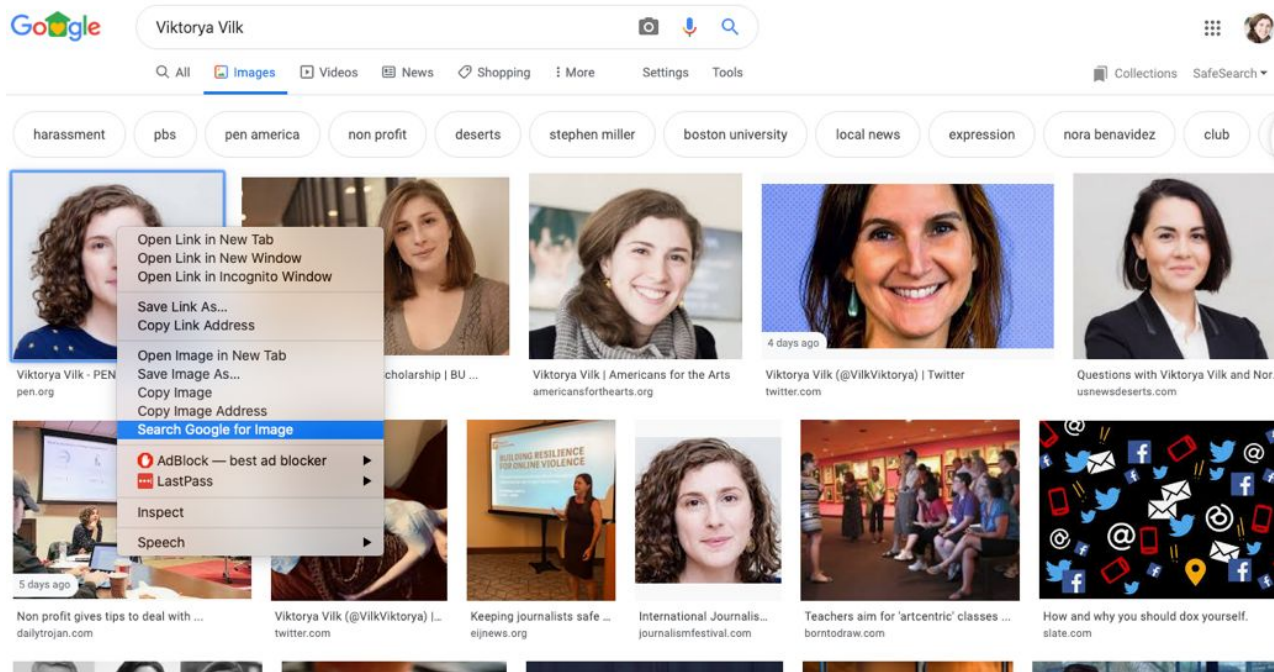
Search for yourself!

Periodically checking to see what results about you populate Google is a great idea



Search engines

Reverse image search



Search engines

Try these advanced search techniques

"Rose Duper" OR "readelev"

Use quotation marks to search for an exact word or set of words. Search different combinations of your name, frequent usernames, phone numbers, and email addresses.

"Rose * Duper"

The asterisk acts as a placeholder for any wildcard terms, for example your middle name or initial.

"Rose * Duper" -site:slate.com

This will exclude results from Slate, showing results otherwise buried in later pages.

"rosecduper@gmail.com" filetype:pdf

This will show any PDFs listing your personal email, for example CVs, alumni publications or past presentations.

Rose Duper site:reddit.com

Search specific sites to find results not indexed by search engines.

Where did all that data come from?



Vector 3: Data brokers

Data brokers

These firms monetize your personal information for sale to advertisers and other bad actors.

These days, they are a dime a dozen:

- Spokeo
- Anywho
- Nexis
- White Pages

Data brokers

Opting out

You can manually opt out of most data brokers, but it can feel like information whack-a-mole.

For help, here's a great cheatsheet by Yael Grauer called the **“Big Ass Data Broker Opt-Out List”**

<https://github.com/yaelwrites/Big-Ass-Data-Broker-Opt-Out-List>

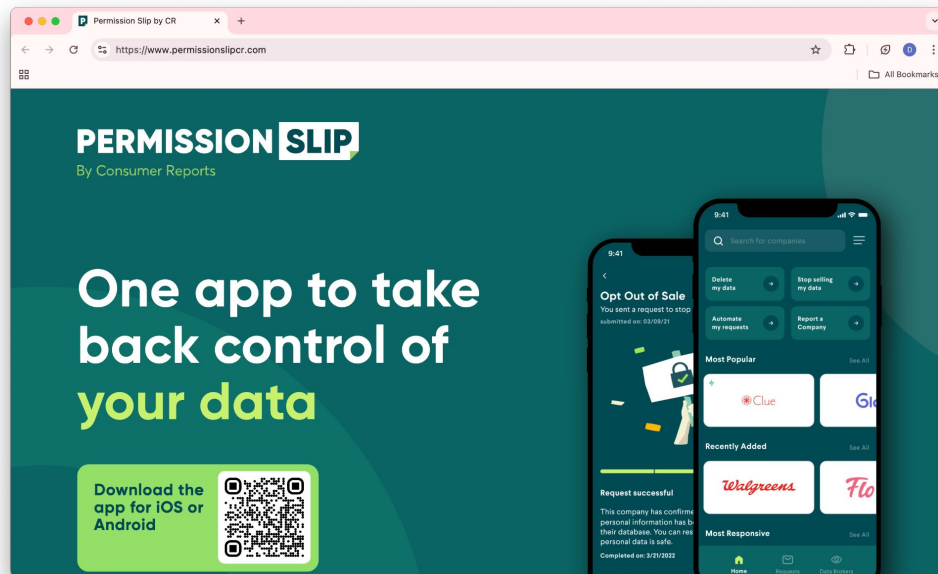


Data brokers

Opting out

As an alternative, invest in a data scrubbing service to handle the opting out for you

Consider Permission Slip from Consumer Reports



Data brokers

Opting out

As an alternative, invest in a data scrubbing service to handle the opting out for you:



joindeleteme.com



optery.com/



thekanary.com/

Questions?

Responding to online abuse

Threat assessment

Ask yourself (w/ a trusted friend or colleague):

Know your harasser?

Especially if history of erratic behavior or violence

Direct, specific threats (name, time, place)?

Intent and Capability

Stalker-like “course of conduct?”

Repeated surveillance and/or threats

Indicia of irrationality?

Not trying to hide (real name, email, phone #)

Online conduct that migrates offline?

e.g. physical mail, threatening voicemails

Professional Liability?

Including non-consensual intimate images

Document the abuse

1. Save a screenshot of the attack
2. Record the following information

Date and time	Attacker's user details (handle/username, real name & posting location if available)	Type of communication (DM, comment, etc.)	Location of incident (URL)	Description of the incident

Mute, block, report

It's a personal choice. Some things to consider:

Mute

Muting someone prevents you from seeing their posts. Someone you mute will not know that you muted them on almost all platforms.

Block

Blocking someone prevents them from being able to engage with you on that platform, however a risk is that they will see they are blocked.

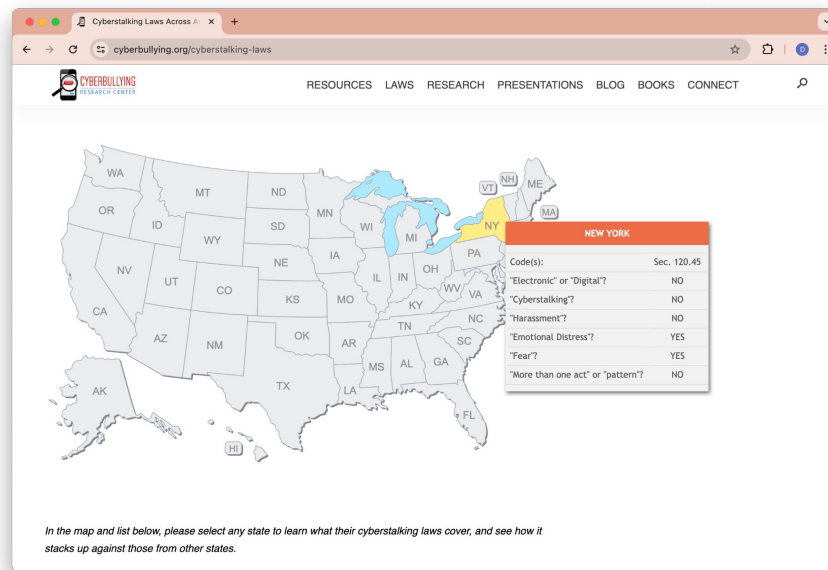
Report

Reporting abuse to the official support or content moderation team on the platform where it happened can help escalate the issue.

Reporting to law enforcement

It's a personal choice. Some things to consider:

- If you decide to contact law enforcement, consider bringing along an ally for support
- Much of the burden of proof lies with those who are suffering from online abuse; be aware of federal and state laws that apply to your situation



Source: cyberbullying.org

Seeking assistance

There are organizations who are prepared to help



**Consult In-House Lawyer
OR Lawyer via NGOs**



**International Legal
Rights Guide**

safetyofjournalists.trust.org/



**US Legal
Considerations**

bit.ly/2kFpBmf



The Freedom
to Write

ONLINE HARASSMENT FIELD MANUAL

[PREPARE](#)[RESPOND](#)[SELF-CARE](#)[LEGAL CONSIDERATIONS](#)[SUPPORT](#)[LEARN MORE](#)

Writers and journalists are facing unprecedented levels of online hate and harassment.

While there are no easy answers, this digital Field Manual contains effective strategies and resources that writers, journalists, their allies, and their employers can use to defend against cyber hate and fight online abuse.



I am a writer/journalist



I am a witness/ally



I am an employer of writers/journalists



FREEDOM OF THE
PRESS FOUNDATION



PEN
AMERICA

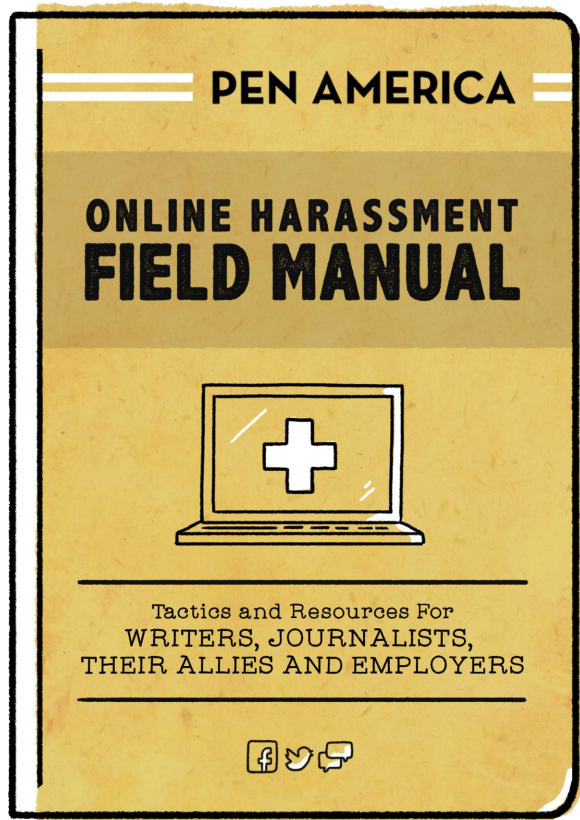
Resources

Check out this guide for a refresher

bit.ly/socialmedialockdown



Questions?



Thank you!



**FREEDOM OF
THE PRESS
FOUNDATION**

Tat Bellamy-Walker
tbellamywalker@pen.org

Davis Erin Anderson
davis@freedom.press