



digital defense fund

Online Harassment & Doxxing Response

Last updated 1/20/21



Hollaback! ✓
@iHollaback



Harassment of any kind is NEVER your fault. We all have the right to live a life free of harassment.

[#TeachMeTuesday](#)

***HARASSMENT OF ANY
KIND IS NEVER YOUR
FAULT. WE ALL HAVE
THE RIGHT TO LIVE A
LIFE FREE OF
HARASSMENT.***

#TEACHMETUESDAY



A quick note on physical vs. digital security

- This presentation will focus on digital security
- Make sure you pair this work with a physical safety plan as well

A quick note on physical vs. digital security

- This presentation will focus on digital security
- Make sure you pair this work with a physical safety plan as well
- A physical safety plan can include:
 - A security team, if you have access to one via your employer
 - Familiarizing yourself with the entry security, guest procedures, and policies of your workplace and the building you live in
 - Safe place ready to go if you need to leave your home
 - A home security system
 - Support network of neighbors and friends
 - For more information about securing your home, we recommend the [“Physical Security Assessment” episode](#) of the Privacy, Security, & OSINT podcast & the [accompanying guide](#)

Doxxing & Harassment Response



Doxxing & Harassment Response Steps

1. Make a physical safety plan
2. Document before you delete
3. Tell your friends & family
4. Block the bad actors
5. Lawyer up
6. Self care

Physical safety first!

Quote from Michelle Ferrier, founder of Trollbusters:

“All the threats are “real”. Anytime someone makes a threat that intimidates or scares you is real, and has a real emotional and psychological impact.”

Suggestions for physical safety from Michelle Ferrier (Trollbusters)

Solve for the physical safe space.

This could mean:

- Telling neighbors & friends so they can keep an eye out.
- Installing a home security system.
- Having a safe place you can go to if necessary (a hotel or a friend with a spare room, for example).
- Asking a friend to come stay with you.



We are not the experts on physical security - but others are!

- For more information about securing your home, we recommend the [“Physical Security Assessment” episode](#) of the Privacy, Security, & OSINT podcast & the [accompanying guide](#)



Is the threat actionable?

Treat all death threats as actionable.

Police sometimes use these questions to evaluate the severity of the threat:

- Is the threat specific?
 - time, place, names
- Do you know the person making the threat?
- Do they have a history of escalating violent behavior?
- Has it migrated from online to offline?
 - For example, are you getting packages or are people showing up where you live/work/travel?



Document before deleting comments

Resist the urge to delete material that is potentially crossing the line into threats.

Be sure to screenshot & download & document as much as possible before deleting these kinds of comments (or before the bad actor deletes their abusive comment).

Documenting for a variety of responses

You will likely need to show documentation of these messages if you choose to escalate any actions to:

- a police report, FBI report, or other legal response
- contribute them to a database of bad actors
- report them to the platform.

Regardless of whether you can or want to rely on the police for assistance, documenting evidence is important!



Instructions on collecting evidence:



- C**ONTACT INFO & DATE
- C**OMplete CONTEXT
- C**ONTROL POSTS
- C**ONFIDENTIAL STORAGE

©
C.A. GOLDBERG
ATTORNEY AT LAW

Incident Tracking Chart

Name of Offender: _____ (if known)

Date & Time of Incident	Method of Contact	Description of Incident	File Name of Screenshot or Voicemail

<http://www.endtechabuse.org/>

<https://www.cagoldberglaw.com/incident-tracking-chart/>

Delegate, delegate, delegate

While you are dealing with harassment, can you delegate managing the messages and comments on your (professional or personal) social media accounts?

Share the resources on documenting threats from the previous slide to make sure the person you delegate can confidently save evidence as they manage your account.



Documentation proves escalation.

Remember escalation paths?

Documentation helps show that one person has made increasingly serious threats, which can help you know when to take action, loop in law enforcement or community safety groups, etc.



Tell your friends & family

We are in the business of stigma busting! It's not your fault, and being harassed is nothing to be ashamed of.

- Let friends & family know you are being targeted
- Tell them to watch out for fake or imposter communications from you and decide on a reliable way to communicate (Signal, phone calls, etc)
- Tell family and friends to be on high alert for potential scams, phishing emails, or threats and to document any scams or threats they receive



Tell your friends and family!

- If you can safely tell your neighbors, landlord, or building manager/security, let them know and enlist their help to keep an eye out for your safety
 - Make sure you have a way to communicate if they see anything sketchy in the neighborhood/your building
- If you have children:
 - Check in with your children's school around their existing campus security procedures.



Give friends & colleagues ways to help!

Some of these tasks can be overwhelming or just downright scary for the person experiencing a doxxing threat or attack.

- Share these resources with them and ask them to protect themselves as well.
 - An attacker may try to get to you by getting to your close connections. If they want to protect you, they should also protect themselves!

Give friends & colleagues ways to help!

- Delegate: Ask someone to help document harassing emails, tweets, comments, etc
- Ask a friend to be the main contact for people outside your core group, so you can focus on yourself & your loved ones
- Have a colleague look up the harassment & reporting rules for social media accounts, or any other information you need to take action



Block, block, block!



Block or report a harasser:

Facebook	https://www.facebook.com/help/290450221052800/
Twitter	https://help.twitter.com/en/using-twitter/blocking-and-unblocking-accounts
Instagram	https://help.instagram.com/454180787965921
Snapchat	https://www.wikihow.com/Block-Someone-on-Snapchat
LinkedIn	https://www.linkedin.com/help/linkedin/answer/47081/blocking-or-unblocking-a-member?lang=en
Gmail	https://support.google.com/mail/answer/8151?co=GENIE.Platform%3DDesktop&hl=en

Lawyer Up!

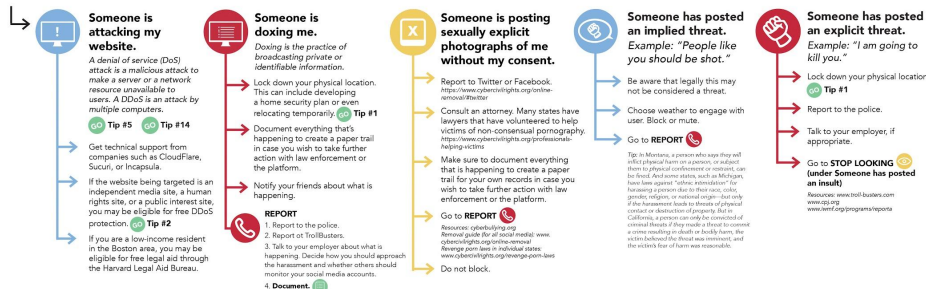
- If you have access to a lawyer or legal team through your work, ask if they can assist in these cases.
 - If not, find a private lawyer with whom you can establish a relationship now, before you need one.
- The legal team can also review comments you aren't sure about.
- It helps often to ask a teammate or friend to go through these for you to ensure you don't have to deal with abuse. Make sure your lawyer/legal team know who that person is.

Bookmark the Trollbusters Flowchart

ARE YOU BEING HARASSED ONLINE?

TrollBusters provides online pest control for writers, journalists and publishers. Report to www.troll-busters.com. If you are not a journalist, check out our Resources for more tips and information.

Step 1: What is happening right now?



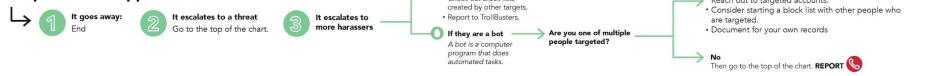
- * Things to document
 - Number of threats.
 - Details (date, time, picture of threat).
 - Number of people involved.
 - Severity of the attack (implied/explicit).
- * Twitter Settings
Change Twitter settings to ensure you only see what you want.
 - You can filter tweets by only people you follow, which means that you'll only see notifications from those accounts.
 - Twitter also has a quality filter, which filters out lower-quality content from people you don't follow and have not recently interacted with.
 - In addition to being able to mute or block users, you can also mute specific words.
 - If you choose to filter or block your tweets, you may want to have someone check the offensive accounts to see if threats against you have escalated.

For instructions on these features and how to use them, see <https://support.twitter.com/articles/1619298>.

- * Who to contact as a student
If you are a student, contact the Student Press Law Center, and report any incidents to your faculty adviser, if appropriate.



Step 2: What happened next?



TROLLBUSTERS
Copyright 2017 All Rights Reserved
Report to troll-busters.com




<https://yoursosteam.wordpress.com/what-to-do-infographic/>



Someone is doxing me.

Doxing is the practice of broadcasting private or identifiable information.

Lock down your physical location. This can include developing a home security plan or even relocating temporarily.  **Tip #1**

Document everything that's happening to create a paper trail in case you wish to take further action with law enforcement or the platform.

Notify your friends about what is happening.



REPORT

1. Report to the police.
2. Report to TrollBusters.
3. Talk to your employer about what is happening. Decide how you should approach the harassment and whether others should monitor your social media accounts.
4. **Document.** 

Self care & community care

From Michelle Ferrier, founder of Trollbusters:

“All the threats are “real”. Anytime someone makes a threat that intimidates or scares you is real, and has a real emotional and psychological impact.”

Trust Your Gut - Extreme Messages

Legislators' offices, nonprofits, and other workplaces often receive extreme communications that don't cross the line into "threat" but still may give you pause.

- Make a log of these communications, a timeline with dates, key phrases, and whether the sender is previously prone to high volumes of calls or letters.

Ensure your coworkers/staff know about these frequent messages, even if you feel silly bringing it up. They may have additional context, or can help you keep an eye out for escalation.

We often have the urge to "be polite" or "not be a bother" but you do not have to deal with disturbing calls or messages alone.



Final Note

It might go without saying, but we like to remind everyone to **trust their gut about an interaction or message feeling "off."** Your instinct built from your expertise and experiences with your work, your space, your community, is one of the most irreplaceable assets in best security practices.

What has worked for you, both for handling threats and taking care of yourself?

