

Managing Cyberhate & Harassment

Sections

- 1 Basic Steps to Mitigate Online Harassment
- 2 Best Practices for Reporting Hate to the Platform
- 3 Documenting the Offensive Content
- 4 Don't Engage with the Harassment (if That is a Real Option for You)
- 5 Services to Manage and Mitigate Harassment
- 6 Tell Your School or Employer
- 7 Preventing Online Attacks
- 8 Online Harassment Glossary

BASIC STEPS TO MITIGATE ONLINE HARASSMENT

Welcome to ADL's online harassment help and resource guide. We know online harassment can be a scary and alienating experience, and we want to ease that pain as much as we can. If you feel you are in danger, contact law enforcement.

If you are being harassed online, know you are not alone. This harassment is not a reflection of your self-worth.

Step back and try to envision the outcome you want and try to proceed with that in mind.

Depending on the outcome you are seeking, you can:

1. Document the harassment by taking screenshots and saving web addresses.
2. Report the harassment to the platform. Include as much information as possible in a single report; don't forget to mention the historical context of

the harassment. Save any case numbers, claim numbers or correspondence you receive from the platform.

3. Try to stop the harassment through blocking and muting users and disengaging from the conversation. Block and mute buttons are usually hidden to the right of the post within a grey arrow, three dots or three lines. You may have an impulse to engage, but those interactions usually go poorly and prolong the issue.
4. If you feel like you are in danger, call 911 and/or file a report with the FBI Cyber Incident Reporting.

BEST PRACTICES FOR REPORTING HATE TO THE PLATFORM

Reporting hate

Every platform is different. This section lays out general best practices, but you may have to look for specific functions or information on each platform separately.

Most online platforms like Twitter or Facebook have built-in mechanisms that allow users to report offensive content or harassment. Reporting mechanisms can usually be found in the three dots, three lines or small arrows that indicate a drop-down menu. The dots, lines, and arrow all indicate that more functions are hidden within. Use the reporting mechanism to report as many pieces of related, hateful content as the platform allows. For example, Twitter allows you to report up to five tweets at once.

If there is no way to report a post through a platform's system, look for the platform's contact information and email them directly.

What to write when you report online hate

All platforms have a terms-of-service (TOS) agreement. Most TOS claim that they do not tolerate hate speech or harassment on their platforms, and you should feel free to ask the company to enforce its TOS. The following page is a compilation of popular companies' terms of service agreements and links to their compliance and reporting sections.

It's useful to understand how the reporting process works from the platform's point of view. Most complaints are handled by a mix of human reviewers and automated moderators. Harassment is often contextual and coded, making it hard for a computer to detect and for human reviewers to recognize. Many reviewers miss the significance of a post because they do not understand the cultural relevance or context of hate speech. When you report offensive content, explain why or how it is offensive. Do not assume the reviewer will understand the post in the same way you do, even if it seems obvious.

Please report the harassment to the platforms before you contact ADL, schools or employers, because you will need the documentation and case numbers for reference. It also helps to show that you have taken the initiative to address the problem before asking for support.

DOCUMENTING THE OFFENSIVE CONTENT

We know it is emotionally difficult and time-consuming to document the harassment. However, putting in the time and effort to take screenshots and save all the content helps when reporting the harassment to platforms, tech companies and law enforcement. Think of this as gathering evidence. Even if the harassment you experience seems obvious and pervasive to you, you will still need to prove that to other parties. The more information you have, the easier it is to demonstrate what you've been through. If you are being bombarded with offensive

content, ask friends or family members to help you go through and compile the material.

DON'T ENGAGE WITH THE HARASSMENT (IF THAT IS A REAL OPTION FOR YOU)

Many organizations advise people to block and mute the offensive users. We know this is not going to solve the problem of online hate, but it might make your online life more pleasant. Engaging with trolls or harassers, or even people who have just left one mean comment, often develops into an online shouting match and does not help anyone. The trolls continue to act because they are getting a reaction, but they are not likely to learn anything about a topic from the interaction.

However, just staying off the internet is clearly not a solution, especially since so many careers depend on having a public presence. It's also deeply unfair to ask the victims of cyberhate – and not the perpetrators – to vacate the public sphere. Asking people to retreat into hiding is not a solution to online hate. But be aware that engaging with cyber harassers often leads to an escalation of hatred rather than a thoughtful dialogue.

Our advice is to assess your personal situation and proceed with caution. For more details, check out the following article from Pen America.

SERVICES TO MANAGE AND MITIGATE HARASSMENT

It can be retraumatizing for those who have been targets of larger scale and coordinated attacks to clean up the mess of unwanted emails or social media posts. Research shows that many people give their passwords to trusted friends and family so they can comb through the messages, documenting and deleting as necessary.

For email attacks, try Squadbox, which streamlines the process of letting trusted third parties clean out an email inbox.

For doxing and campaign attacks (when your personal information has been released online), contact Crash Override Network. Crash Override has an online abuse crisis helpline, resource center and advocacy group staffed by survivors.

For Non-Consensual Intimate Imagery (Non-Consensual Pornography), contact the Cyber Civil Rights Initiative or call the hotline for help removing the content and legal resources.

For Intimate Partner Violence or if you are being stalked online by a current or former partner please reach out to the National Network to End Domestic Violence for a resources and a helpline.

For specific threats or if you feel unsafe, please contact local law enforcement.

To resolve an issue with a platform, contact the platform and then ADL.

If you have already reported the hateful content to the platform and they have not taken action, and you are being personally targeted or the content will have wide-reaching consequences, please report it to ADL.

What can ADL do for you?

In most cases, the harassment can be addressed by the targeted person. However, when cases are too much for one person to handle, ADL and other organizations can help. Please check out our Online Harassment Glossary for an explanation of what you may be experiencing.

Our primary goal is to help people who have been targets of any kind of hate, bias or harassment in any way we can. In cases of harassment, we can communicate with the tech company on the victim's behalf if the victim has also reported the online hate to the company and not received help.

What can you expect from ADL?

We cannot remove all hateful content from the internet. However, if someone is being targeted for harassment and the platform has refused to act, please report it to us on our incident response form. Even if you do not need our help, we appreciate you reporting the event to us, as it helps us assess the state of online hate.

If you report a case that we can help with, a representative from your region will contact you. Everything you share will be confidential.

We can't say this enough: If you feel like you are in danger or this rises to the level of a crime, contact local law enforcement and the FBI Internet Crimes and Complaint Center.

TELL YOUR SCHOOL OR EMPLOYER

If the harassment is related to employment or school, tell the employer or school. Even if they claim they cannot do anything about the incident, make sure they know about it and document the fact that they have been informed. We believe schools and employers have a responsibility to address bullying and harassment related to school and workplaces and should be encouraged to take action.

ADL and the federal government believe schools should act to address cyberbullying. Online change will come from changes in people's real feelings and attitudes. We must instill a love of diversity in students through anti-bias work at the school and household level. Spewing hate is a learned behavior that can be encouraged or discouraged by peers and institutions.

Students who make hateful comments online often begin slowly, or in person, and continue or stop the behavior based on the reaction of their peers. If the student receives a positive reaction to hate, the statements become more extreme and more frequent. If action is taken by school, parents, colleagues, friends or online communities that make it clear that bigotry is not acceptable, students learn not to engage in these behaviors.

If you would like to bring anti-bias education to your school, please check out our free anti-bias program for schools, [No Place for Hate](#).

Likewise, workplaces with public-facing employees should take care to make sure their employees are safe at all times.

PREVENTING ONLINE ATTACKS

Take a Course in Security and Cyber Safety: [TrollBusters](#) offers courses in security and mini-lessons (5-10 minutes each) on cyber safety (for instance, writing strong passwords and using two-factor authentication).

Read Up: We like [Hackerblossom's Guide](#) to Feminist CyberSecurity for their thoughtful and thorough approach.

Other approaches to try:

- Use a third-party service like TrollBusters' [Social Media Monitoring](#).
- Protect your privacy by using a virtual private network (VPN). [See VPN reviews here](#).
- [Remove your name and contact information](#) from any and all online white pages and other online directories.
- Use a webcam and microphone cover: cameras and mics on digital devices are relatively easy to break into. A piece of tape or a post-it is usually sufficient, but high-quality adhesive covers are available at many stores and online.

ONLINE HARASSMENT GLOSSARY

Online harassment and offensive content runs the gamut from individual hate-filled posts to bullying, stalking, doxing and campaign harassment. It might be helpful to check out the charts and figure out what kind of harassment you are experiencing. It's also helpful to know the terminology when reporting the offense to the platform, school or employer.

You can check ADL's list, or see the list and recommended steps in this great infographic from TrollBusters.

- [Online Harassment Chart](#)

Online Harassment Glossary

Online abuse is a continuum of tactics that range from bullying, harassment and trolling, to stalking, violence and coordinated attacks. It's useful to know what kind of harassment you are facing when deciding how to combat the problem. Below you will find definitions of general harassment strategies and specific harassment tactics.

Cyber Harassment Styles

Cyberbullying: Cyberbullying refers to bullying, especially among youth, that takes place through online means such as social media. The bully repeatedly communicates hostile or aggressive messages intended to inflict harm or discomfort onto others.

Bullying includes physical, verbal and relational abuse, which harms the social, physical and psychological health of both the bullies and their targets. Bullying usually involves repeated negative actions that *create a power imbalance between perpetrator and victim*, although not all studies conclude that the action must be repeated to constitute bullying.

For young adults, cyberbullying is most likely to take place through social media and texting.

Cyberstalking: *Cyberstalking refers to threats and harassment to a particular individual that cross the border between online and offline. Cyberstalkers are usually driven by anger at a specific person, in contrast to trolls who harass for fun.*

Cyberviolence: Aggressive forms of online abuse are best understood as cyberviolence — that is, harm perpetuated through online or digital means, especially based on sex and gender. It encompasses online harassment and abuse, usually directed at women, girls, sexual or gender minorities, and intimate partners. Cyberviolence often overlaps with cyberstalking and intimate partner violence, and may cross from online to offline. Cyberviolence, like cyberstalking, often correlates with offline violence and abuse.

Campaign Harassment: Many incidents of harassment involve numerous perpetrators working in concert, contrary to the stereotype of the lone anti-social troll. The term “campaign harassment” describes distributed, networked efforts to harass, intimidate, threaten and silence victims. Such campaigns typically target

women, celebrities, people of color, academics and journalists.

Harassment in Gaming: A major subset of cyber harassment takes place in online gaming, especially immersive MMORPGs (Massively Multiple Online Role-Playing Games, like World of Warcraft). Many methods of harassment deployed in gaming later spread to general cyber harassment.

Cyber Harassment Tactics

Verbal abuse: The most common form of direct harassment most people witness or experience is verbal abuse. Verbal abuse includes name-calling, slurs, threats (often graphic), humiliation and flaming (aggressive verbal attacks/arguments). Verbal abuse can take place in view of others, as on social media and in comment sections, or privately via email, text or chat. Verbal abuse can multiply when numerous attackers (or multiple online identities for one attacker) target a victim *en masse*.

Defamation: False statements intended to damage or harm someone's reputation, such as lies intended to get someone fired.

Deadnaming: Calling a transgender person who has transitioned or adopted a new name by their prior given or legal name, especially with the intent to out them or undermine their identity.

Denial of Access: Using tech tools or features to overwhelm a service, site, personal account or server. Attacks, which are often distributed across a large number of users and/or devices, may send excessive unwanted messages to make an account unusable, execute Distributed Denial of Service attacks (DDoS) against a web server, generate tweetstorms or submit many requests to block or report targeted users. Denial of access can also include seemingly innocuous messages that take up a target's time, sometimes called "sealioning".

Doxing/Doxxing: Publishing private, identifiable information about a victim, such as a name, address, personal email or phone number, which enables in-person stalking, harassment, threats and violence.

Flaming: Virulent verbal attacks in an online forum, often as part of an argument. Relates to flamewars, incendiary online debates or fights (which are not necessarily initially a form of harassment).

Griefing: In online gaming, “griefers” are uncooperative players. They can obstruct desired goals in multi-player game environments by repeatedly killing players, interfering with building or destroying works made by other players.

Hacking: gaining access to someone’s computer, stored files or accounts on their own or third- party services.

Happy slapping: Using a mobile device to record or film abuse or an attack.

Impersonation: Pretending to be the target by creating accounts in the target’s name or using the target’s domain, often to harass, insult or intimidate others, seemingly on behalf of the target.

Pranking: Mainly a tactic of trolls, pranks can involve tech tools like hacking to target a website or an individual. While pranking may appear simply mischievous, it can have harmful consequences for victims, and often targets vulnerable or marginalized people. For example, in 2008, hackers hijacked the Epilepsy Foundation’s website and flashed images, inducing at least one epileptic seizure in a site visitor.

Meme abuse: Using memes, especially hateful, violent or offensive ones, to harass or abuse someone.

Sexting: Sending sexually explicit text messages as part of abuse (sexting is

typically not abusive, but can be used in a campaign of partner/dating abuse or harassment).

Shaming: Harassment based on a person's violation of a perceived social norm.

Swatting: Falsely reporting a crime at someone's address to send a special police (SWAT) team to investigate, which can result (and has resulted) in violence or death.

Tracking/monitoring: Using GPS to track and surveil a targets' movements and communications.

Trolling: The meaning of trolling has transformed over time, from intentional provocation of individuals in online communities, especially new members, to more generalized disruptiveness and harassment, aimed at strangers or public figures, often according to specific categories of identity.

Non-consensual distribution of intimate images: Sharing or distributing sexually explicit images of someone online without their permission. Sometimes referred to as "revenge porn".

Vandalism: Digitally defacing a website or other online medium.

A Note on Trolls

As Troy McEwan explains in *The Conversation*, "trolling is acting in deceptive, disruptive and destructive ways in internet social settings with no apparent purpose". According to a 2017 study by Justin Cheng et al., however, what constitutes abusive or disruptive behavior depends on the norms of a given forum or community: "behavior outside the acceptable bounds defined by several community guidelines for discussion forums". What counts as trolling, in other words, depends in part on the norms of the social milieu in which the activity is

pursued. The often fuzzy border between good-natured joking and malice is a feature of this style of harassment.

Social scientists have attempted to identify the motivations for this behavior in cases when it is not directed by hate. For many trolls, the aim is to control an online social space or to seek amusement through their harassing or disruptive behavior. For example, a review by psychologist Mark Griffiths similarly describes trolling as “an act of intentionally provoking and/or antagonizing users in an online environment that creates an often desirable, sometimes predictable, outcome for the troll”.

A study of trolling on Wikipedia by Shachaf and Hara found that trolls are motivated by boredom, attention seeking and revenge, causing intentional harm not only to other users but to the site itself. Other research, such as the 2017 study by Cheng et al., finds that trolling behavior depends not solely on personality traits, but setting and context, concluding that “ordinary people can, under the right circumstances, behave like trolls”.