Investigating Digital Abuse:

Mitigating Harm Online and on The Ground

A TOOLKIT FOR LAW ENFORCEMENT

ADL®
FIGHTING HATE FOR GOOD

Table of Contents

Executive Summary

This toolkit is a brief primer on the most salient and common issues that law enforcement may face while responding to incidents of digital abuse, as well as best practices on how to address them.

Online harassment and abuse pose serious threats to individuals, communities, and society—rising in pace with advances in digital technology worldwide. This abuse comes in many forms, generally marked by an intent to intimidate, threaten, or bully a person or group; to undermine trust by sharing harmful false information; or to incite harm against a person or group.

Digital abuse occurs in online spaces across digital communication platforms–social media, email, messaging apps, and blogs and websites. But too often harm extends beyond the screen and into the offline world. Digital abuse has severe negative impacts on victims, such as emotional distress, reputational and financial damage, physical harm, and even death.

Despite the real-world dangers that digital abuse poses, many victims fail to reach out to law enforcement, often because they feel shame, fear being blamed, or are concerned about retaliation by their abusers. Due to the speed with which technologies develop, law enforcement agencies must constantly adapt to new forms of threats and the ways that they can occur, while being aware of the substantive and procedural legal concerns involved.

Law enforcement agencies can play a critical role in addressing digital abuse and reducing its harm. They are often the first line of defense against bad actors, and their actions can help make victims of online abuse safer.

What is in this toolkit?

This brief toolkit covers the most common issues law enforcement may encounter when responding to cases of online abuse. We hope it equips law enforcement officials with helpful tools to approach cases of online harm and to help reduce their negative impact.

While not a comprehensive resource, this toolkit provides recommendations and best practices for addressing reports of digital abuse effectively, from recognizing digital abuse as it occurs to building effective rapport with victims, collecting relevant evidence, and identifying identity-based hate. It is intended to help law enforcement agencies do their part to promote safer online spaces for all.

Why now?

With the rise of online harassment and abuse, law enforcement agencies are the first line of defense against bad actors: they are essential to supporting victims and pursuing accountability for harms. While there are resources designed with victims of online harm as the intended audience, this toolkit is specially tailored to a law enforcement audience and describes the role that law enforcement can play in responding to threats and establishing trust with victims during their time of need.

Disclaimer

Each law enforcement agency will be bound by different municipal, local, or state codes, laws, policies, and guidelines, which may affect how suggested principles in this toolkit can be best utilized or implemented. It is imperative that each agency seek legal and professional guidance to ensure full legal and policy compliance in accordance with state law and agency guidelines. This resource is not intended to and does not provide legal advice.

Terminology: Common Digital Abuse Tactics

- **Cyber Harassment: Engaging in electronic communication that harasses, terrorizes, or threatens an individual or group, often on the basis of their identity.** This term is used both to describe individual acts and as an umbrella term to broadly describe types of internet-enabled abuse.

- **Cyberstalking: Using the internet and technology to pursue or stalk another person.** Cyberstalking generally refers to a pattern of online activity, amounting to a course of conduct targeted at or concerning a particular person, which would cause a reasonable person to fear for their safety (or the safety of their family). Cyberstalking includes sending persistent and unwanted messages, tracking someone's location with geolocation technology without their consent, hacking accounts using secretly installed password trackers, and sending a barrage of messages to an individual or their network from fake accounts. At its core, cyberstalking is rooted in the creation of a dynamic that is meant to make its victim feel disempowered.

- **Deep Fakes: The combining of real images, videos, or audio content with machine learning technology to create a new, synthetic piece of media—often with the intent to deceive audiences.** Some examples of deceptive deep fakes include videos of politicians depicted in situations that never happened, or fabricated pornographic videos targeting specific individuals. Deep fakes of all kinds could lead to serious forms of fraud, identity theft, and in certain cases, the spread of harmful disinformation. In recent months, rapid advances in generative artificial intelligence have exacerbated the threat that deep fake technology poses to trust and individual safety alike.

- **Doxing** (also known as 'doxxing'): **Broadcasting of private or identifying information about an individual, group or organization with the intent of causing harm.** The information shared could be a person's full name, address (or the addresses of their loved ones), phone number, email address, social security number, or other sensitive data. It can similarly involve sharing information about an individual's family or place of employment, or otherwise sharing private information and encouraging others to leverage this information to engage in harm.

- **Nonconsensual Distribution of Intimate Imagery** (NCII): **Also known as image-based sexual abuse, nonconsensual pornography, or "revenge porn." This is defined as the distribution of sexually explicit images of individuals or depicting individuals in a sexually explicit manner without their consent.** Some examples of NCII include the dissemination of sexually explicit images of a current or former partner; the hacking of a user's device or account to access sexually explicit images; or otherwise gaining access to and distributing sexually explicit images without the consent of the person depicted. NCII has long threatened and posed danger to many victims–most of whom are historically women, people of color, or members of the LGBTQ+ community. Notably, the threat is now made worse by generative AI because this technology can create sexually explicit images of a person without their consent.

- **Swatting: An extremely dangerous, illegal "prank" that involves falsely reporting an emergency (most often a hostage situation, bomb threat, mass shooting or other violent crime) triggering the deployment of a law enforcement unit (usually a SWAT team) to the victim's location.** Swatting wastes significant resources and may prevent law enforcement from addressing real emergencies as efficiently. Cases of swatting have resulted in injuries, and even death to victims and witnesses alike.

- **Zoombombing: The unwanted disruption of video conferences or online meetings–especially via the Zoom platform—often by graphic, hateful or threatening messages, symbols, or noises.** It can lead to the shutdown of important meetings and has posed significant problems for virtual gatherings in educational, religious, and professional settings. Zoombombing can happen when bad actors gain access to an online meeting's link and password, or when they use scanning technologies to find vulnerabilities in a host program's security features.

Trends: Online Hate and Digital Abuse

Online hate and harassment are rampant and can be far more harmful than "awful but lawful" protected speech. It ventures into the realm of unlawful, dangerous speech as well as conduct that can—and often does—cause significant real-world harm. Because our connection to online spaces is ubiquitous and near-constant, victims are seldom able to escape digital abuse by simply turning off their phones or logging off of social media. Considering this reality, strong responses by law enforcement to reports of online hate, harassment and abuse make all the difference in protecting individuals and communities from otherwise inescapable harm.

ADL's research on online hate and harassment shows:

- Over half (56%) of American adults have ever experienced harassment on social media in 2024, up from 40% in 2022. (2024 Online Hate and Harassment Survey)
- 22% of American adults experienced severe harassment in the past year alone, which includes physical threats, sustained harassment, stalking, sexual harassment, doxing, and swatting, up from 18% in 2023. (2024 Online Hate and Harassment Survey)
- 50% of teens 13-17 were harassed in the past year, 61% of this harassment took place on Facebook.
- 74% of teens (ages 13-17) and 75% of pre-teens (ages 10-12) experienced harassment in online multiplayer games. (2023 Online Multiplayer Games Survey)
- Online hate is a problem that causes harm to people's personal and professional lives. ADL's ethnographic study, The Trolls are Organized and Everyone's a Target: The Effects of Online Hate and Harassment, provides personal stories of victims of online hate in an attempt to paint a more complete picture of the ways in which harassment can envelop multiple facets of a person's life. The rhetoric and tactics used in online hatred are often rooted in racism, white supremacy, misogyny, homophobia, and antisemitism.

- Incidents of online hate and harassment are frequently connected to a victim's identity. When investigating an incident of online hate or harassment, it is important to consider whether there is, or could be, a hate or bias motivation. (2024 Online Hate and Harassment Survey)

Questions to consider when assessing possible identity-based hate incidents:

1. Has the subject made comments about the victim indicating a possible bias motivation, in whole or in substantial part because of the actual or perceived race, color, ethnicity, religion, national origin, gender, sexual orientation, gender identity or expression, or disability?
    - Even if the offender(s) was mistaken in their perception that the victim(s) was a member of the group they were acting against, it can still be bias-motivated if the offender selected the victim(s) because of one of these characteristics.
2. Is there evidence of a possible bias motivation in the perpetrator's social media activity, text messages, or online footprint?

3. Is there evidence of bigotry exhibited by the perpetrator via symbols such as tattoos, clothing, patches, etc.? Refer to ADL's Hate on Display: Hate Symbols Database.
4. Has the victim publicly identified themself or been associated with activities related to identity characteristics, for which they may have been targeted?
5. Is there is a federal, state or local criminal hate or bias statute that may apply?
    - According to federal law, a hate crime is a committed criminal offense which is motivated, in whole or in part, by the offender's bias(es) against a race, religion, disability, sexual orientation, ethnicity, gender, or gender identity. Forty-six states and the District of Columbia have also enacted hate crime laws which vary widely in terms of which aspects of identity are covered, with some states offering much broader protections than others.
6. **Tip:** Even if there does not initially appear to be evidence of a hate or bias motivation at the start of an investigation, keep in mind that as additional evidence is collected, indicators of this type of motivation may surface.

Characteristics: How Online Hate and Harassment Incidents are Unique

Online hate and harassment have the potential to escalate over time, increasing in frequency and intensity:

- Tip: It is important to take each report of online hate or harassment seriously and to collect and preserve as much digital evidence as possible, including but not limited to, precise language, images, or IP addresses. This may include collecting evidence from multiple platforms, and from both the victim and alleged bad actor, as well as from any witnesses, where identifiable.

Online hate is often not limited to the web. In many cases, it has the capacity to spill over into what happens offline:

- Online activity can lead to physical assaults and violence. Suicide is the second leading cause of death for US adolescents and young adults, and many of these cases can be traced to the damaging impact of online abuse on psychological health. Similarly, there may be an online component and digital evidence related to crimes that take place in person.

Online harassment can have both an emotional and economic impact:

- Experiencing severe online harassment can be traumatic, stressful, isolating, and fear-inducing. Economically, it has the potential to damage a victim's reputation and career prospects. There are also costs associated with needing to implement security measures as a result of cyber harassment. In some cases, online harassment even impacts civic engagement. It can chill or stymie attempts at political participation, especially those of women and people of color. Similarly, harassment of journalists has a chilling effect on press freedom.

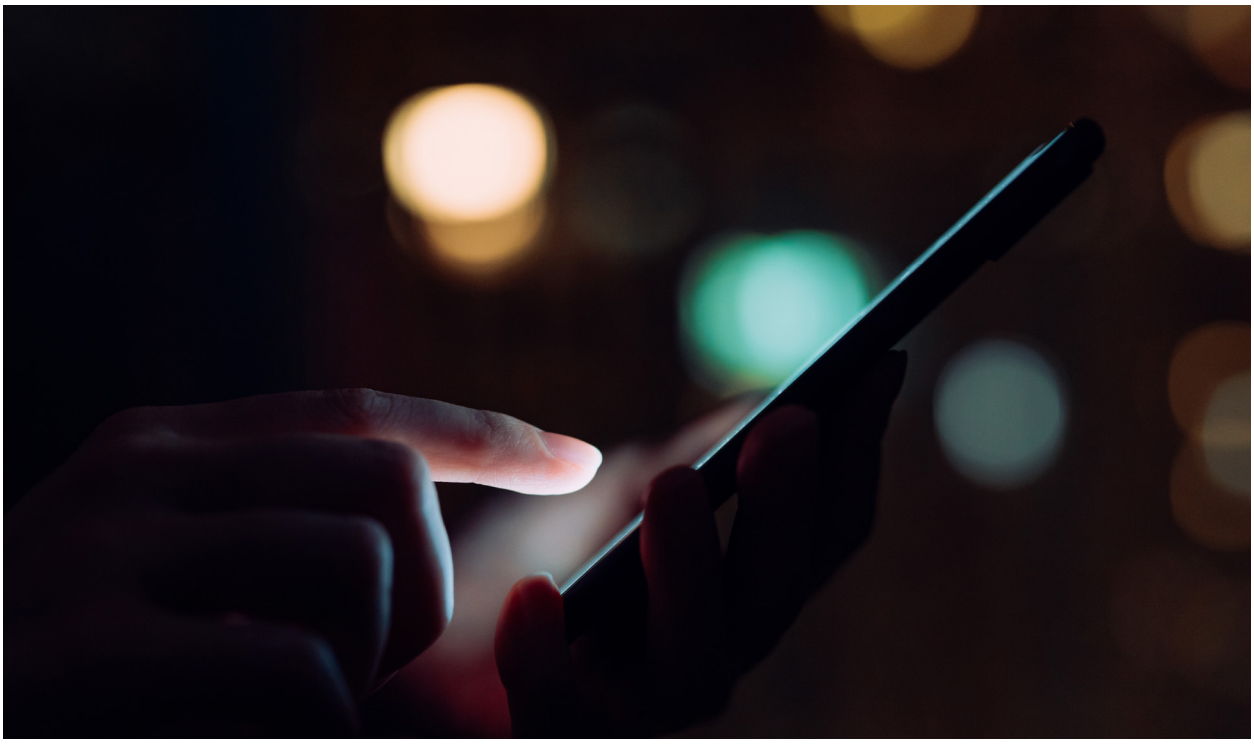
Abuse on Social Media Platforms

Victims experience harassment on a wide variety of platforms:

- This may include mainstream social media (e.g., X, Instagram, Facebook and YouTube), anonymous or pseudonymous web boards (such as 4chan, 8chan and Reddit), gaming and related sites (Twitch and Discord), online review sites (Yelp and Google), publishing platforms (Wordpress, Medium and other online publications), and websites that have been known to spread extreme content (Breitbart, Quillette and Stormfront). Victims can also experience digital abuse and harassment via email, text, and personal messaging apps (e.g., What's App).

Victims more often than not feel dissatisfied by the responses they receive when reporting online hate and harassment to social media platforms:

- Often, platforms do not efficiently review or remove hateful content. It can take weeks for their content moderation teams to respond to reports of harassment. Some reports receive no response at all. Most platform reporting systems are also designed so users can only report one hateful post or account at a time.



Common Tactics for Digital Abuse

Cyberstalking

Cyberstalking is the act of using the internet and technology to pursue or stalk another person. According to a 2019 US Department of Justice report:

- About 1.3% (3.4 million) of all people aged 16 or older were victims of stalking; however, fewer than a third (29%) of all stalking victims reported the victimization to police.
- Women (1.8%) were stalked more than twice as often as men were (0.8%).
- An estimated 67% of victims of both traditional stalking as well as stalking with technology were fearful of being killed or physically harmed

Doxing

Many people define doxing as posting someone's personal information online; however, doxing as a blanket term threatens to ignore the crucial difference between criminal doxing on the one hand, and, on the other, lawfully identifying people online. For the latter, the purpose may be to protect others, track down extremists, or report on a public interest story. ADL would not consider these uses as doxing.

- **Unlawful doxing** is when someone posts personally identifiable information (PII) of an individual and, in doing so, meets specific standards of intent that go to whether the disclosure will lead to criminal conduct (e.g., stalking, bodily injury, or death).
  - PII refers to any information that can be used to identify an individual, either alone or in combination with other data. PII examples include, but are not limited to, a person's full name, date of birth, Social Security number, passport number, driver's license number, bank account information, home address, email address, phone number, or any other information that can be used to uniquely identify or contact an individual.
- **Tip:** Intent to harm is the distinguishing factor when it comes to unlawful doxing. It can often be ascertained clearly by the bad actor's explicit directives to an audience, or in context with the bad actor's other posts.

Notable Statistics on Doxing:

- 21% percent of Americans (over 43 million people) have experienced doxing, while 62% of those individuals personally knew someone who experienced doxing (SafeHome.org).
- Of the types of personally identifying information shared during doxing incidents:
  - 90% of doxed files included the victim's address;
  - 60% included the victim's cell phone;
  - 53% included the victim's email address; and
  - 40% included the victim's IP address.

Swatting

Swatting is the act of falsely reporting an emergency to trigger the deployment of a law enforcement unit (usually a SWAT team) to the victim's location. Swatting origins can be found in online communities associated with gamers and hackers. For example, some gamers targeted their rivals by contacting 911 during livestreams to watch online while a SWAT team conducts a raid on their victims.

Swatting appears to be on the rise:

- Experts have estimated incidents jumped from 400 cases in 2011 to over 1,000 in 2019. Notably, we have seen a surge in serial swatting cases between 2021 and 2023 targeting schools and religious institutions. Unfortunately, the actual number is unknown because the FBI does not track swatting as a unique category of crime, and many local police departments fail to distinguish swatting from false police reports or categorizing many of these as bomb threats.

Swatting impacts law enforcement's ability to protect communities:

- Swatting takes first responders away from actual emergencies, potentially endangering the safety of others.
- Swatting puts victims, responding officers, and other community members in harm's way and sometimes results in deaths.
- Swatting grossly misuses taxpayer dollars. The extent of the financial burden these cases place on taxpayers varies but an incident can cost tens of thousands of dollars.
  - For example, a swatting incident in Rochester, New York was estimated to cost up to $15,000. In Denver, a swatting incident cost law enforcement $25,000, while one in Long Beach, New York is estimated to have cost $100,000.

Legal protections against swatting vary by jurisdiction. In over 1/3 of states, there is no meaningful legal distinction between swatting and prank-calling law enforcement—even though the results can be drastically different and lasting impact can be severe.

.

Agency and Policy Resourcing

It is critical for agencies to be educated on the topic of cyber and digital abuse for a variety of reasons, including addressing potential criminal activity, keeping the public safe, and ensuring that victims of crimes are treated with courtesy, respect and understanding.

How agencies can address digital abuse from a policy and resource perspective:

- Consider establishing a task force, sub-unit or committee on digital abuse to enlist personnel within the agency who may have subject matter expertise. Members of this unit or committee can provide support while conducting investigations to determine whether a crime has been committed.
  - **Tip:** Consider including personnel with specialized unit training, such as hate crimes, special victims, child or elder abuse.
- Provide ongoing training and professional development related to digital abuse. This is critical to ensuring that agency personnel have the education and resources available to them to thoroughly investigate this type of misconduct.
  - **Tip:** Consider implementing "victim-centered" training programs. This may be beneficial for detectives and officers engaging with individuals who are victims of digital abuse.
- Designate a team of investigators within the agency (the number of designees should depend on a department's size and resources) to be points of contact for:
  - Education and guidance on cyber abuse (i.e., new technology, new websites, new or novel ways in which bad actors engage in continued abuse)
  - Community liaisons for proactive outreach to the public.

Questions to consider for improving agency policies and procedures:

1. Does your agency have a social media office?
2. Would awareness of the issue be a topic to consider in the next social media campaign to spread information on the dangers of cyber stalking, cyber abuse, doxing, or swatting?

.

Outreach and Communication with Complainants

It can feel overwhelming to be a victim of harassment, regardless of where it takes place. Victims often report experiencing shame and embarrassment, and fear retaliation if they were to report incidents to the police. In some difficult cases, victims note that even when they finally work up the courage to report abuse, law enforcement's response—for a variety of reasons—does little to alleviate the victim's pressing, legitimate concerns. Notably, incidents of identity-based online abuse and harassment are even more damaging because of the unique message it sends to an individual about their safety and the safety of their intersecting communities.

Robust law enforcement response to victims of digital abuse is essential:

- A knowledgeable, considerate response helps alleviate the emotional and psychological trauma that victims often experience from digital abuse. Knowing that law enforcement is handling a situation with respect and efficacy allows victims of abuse to begin recovering from deeply harmful experiences.

> **"I can't explain it now because it's over, but when you're in the middle of it, receiving rape threats, death threats, on a daily basis, impersonating you. It's hard to reach out for help, and when you do, you get a stock response. It just makes my heart sink."**
>
> — An interviewee from ADL's 2019 report, The Trolls are Organized and Everyone's a Target: The Effects of Online Hate and Harassment

Law enforcement officials are often best equipped to bring bad actors to justice:

- Their resources and understanding of criminal law and process can enable victims to help hold bad actors accountable for the harm they may have committed. Law enforcement response –if sufficiently robust–may discourage bad actors who otherwise potentially engage in acts of digital abuse with no concerns about enforcement or penalties.

Law enforcement officials can normalize reporting online abuse:

- Agencies can foster an environment where victims feel more empowered to speak out against their abusers and pursue the help they need.

Recommendations for Improving Interactions With Victims of Online Harassment and Abuse

1

Be Patient. Not every victim will feel comfortable sharing potentially private and/or embarrassing details of their lives with you. Explain that you will need to ask some potentially uncomfortable questions and that you are not here to judge, but simply wish to get as much information as possible to understand what happened and see how you can help. Practice empathy and make every effort not to be judgmental of victims seeking your assistance during their time of need; many of them have nowhere else to turn for help.

2

Provide context. Explain that you may need access to their cell phone, texts, social media accounts, or email inboxes.

- Give context as to why you might need to access these items and ask for permission to do so. Victims of digital abuse have suffered violations of their consent by default, so knowing that you respect their agency and consent may inspire confidence and trust. **The key here is explaining why the information is helpful, offering victims a choice, and ensuring that they understand how you can help them.** This should be done with legal and agency guidelines to ensure items are accessed with proper legal permission.

3

Stay connected. Encourage victims to reach out if any new developments arise, and especially to let you know if a bad actor escalates or continues to engage in contact with the victim.

- This lets the victim know that you are approachable, open to listening to them, and committed to helping resolve their case. It also assists in investigatory steps to collect more evidence if additional incidents occur. Incidents of online harassment are not usually one-offs. Research shows that victims who are targeted based on their protected identities or know their abuser from a prior relationship are not usually targeted in isolation. Sustained harassment campaigns can also sometimes take place via multiple media outlets, including social media platforms, websites, text messages, and phone calls. Encourage the victim to share openly with you all the ways the bad actor has engaged in harassment.

4

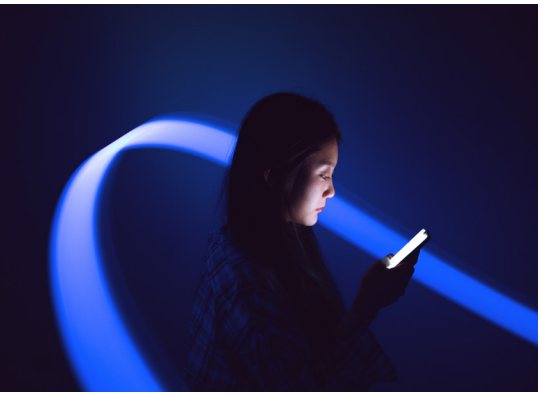
Remain empathetic. When asking questions, demonstrate non-judgment and encourage open-ended responses from the victim.

- Refrain from making comments or asking questions in a way that signals a perception that the victim is at fault (e.g., questions like, *why would you take a photo of yourself naked and send it to someone you never met before?*)
- Refrain from making comments that may be perceived as law enforcement not taking the case seriously or not wanting to investigate (e.g., *Just delete your account and then the harassment will stop, don't go on social media anymore, or it's just online, it's not like anyone hurt you in real life*).
- Remember, most Americans have social media accounts, interact with others on them, and consider them a necessary, inextricable aspect of their daily lives. In the same way we would not encourage a victim of robbery to leave their wallet at home during their next outing, we do not want to chill victims' speech by encouraging them to get offline.

5

Stay in touch. Consider what information you can and cannot share.

- Even if it seems trivial, providing certain points of information to a victim helps them feel like your department is taking them and the investigation seriously. They might simply need to hear that you have filed paperwork, spoken with an additional potential witness, or attempted to secure a piece of evidence. These steps may be routine for you, but for a victim they are not. It is equally important to consider explaining why certain aspects of the investigation cannot be shared with the victim and that these investigations take time.
- Strongly consider checking in periodically, even if there is no change in status of an investigation. A phone call to let a victim know you are still working on their case goes a long way in acknowledging the validity of an incident and your commitment to the pursuit of accountability and justice.



6

Share resources. Ensure that victims are aware of additional tools or resources, either within your agency or externally. Do you have crime victim advocates or external entities, like counseling services, available for support? Targets of antisemitism, extremism, bias, bigotry or hate can report incidents to ADL at https://www.adl.org/report-incident.

7

Be an advocate. Consider outreach and messaging strategies to your communities, which demonstrates that your department takes digital abuse just as seriously as other potential crimes. This works towards increasing the trust needed for you to do your job of protecting the public on a daily basis.

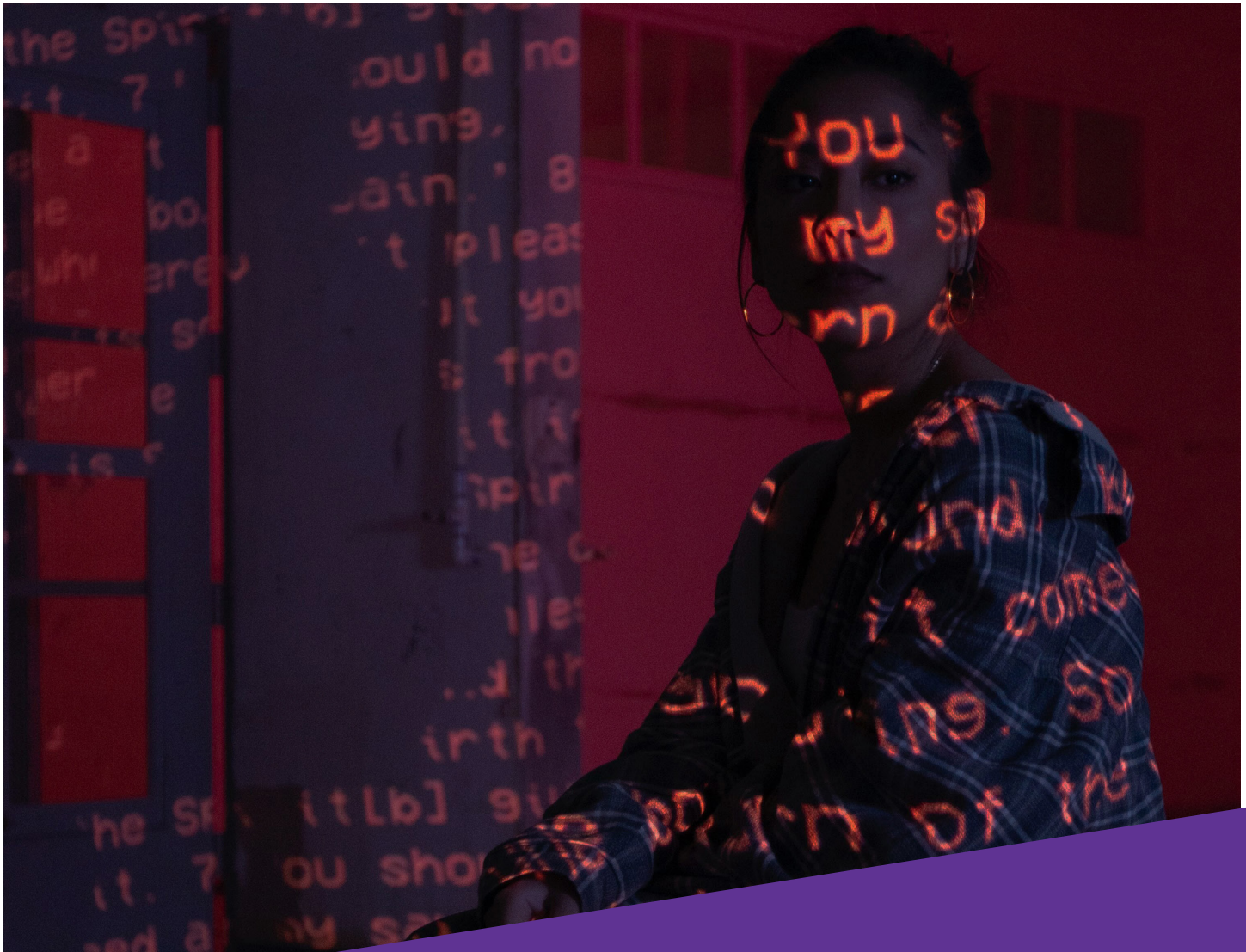
Conclusion

While online spaces and platforms may present challenges initially, the real-world potential for harm against individuals persists. Online harassment and abuse are yet another way bad actors inflict harm which may require law enforcement involvement.

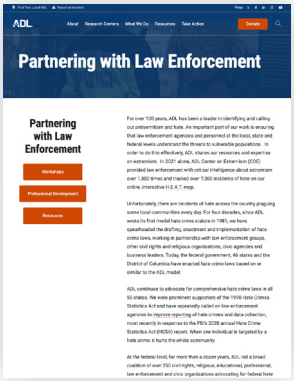
It is incumbent upon law enforcement to take these threats and abuse seriously, treat victims who report incidents with dignity and respect, and demonstrate through their actions that they are there to serve and protect everyone in their community.

These suggested principles should be underscored on an ongoing and regular basis, so that they become part of sustained and positive practices of an agency. Doing so sends a message to communities that their agency takes these incidents seriously and is committed to helping victims who have been targeted by online harassment or abuse — particularly for those within marginalized communities who may be more likely to be targeted via online platforms.

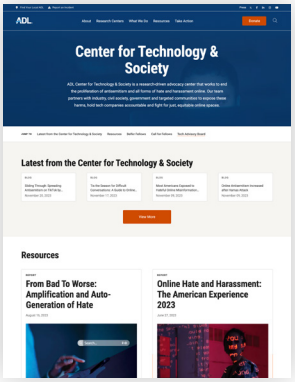
For more information on how ADL can assist and support your agency's efforts in combating online hate and abuse, contact LEResources@adl.org**.**



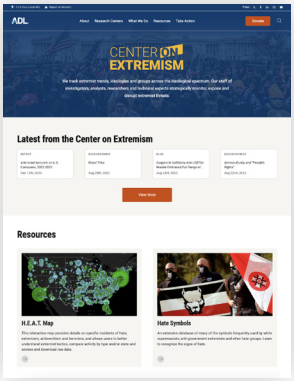
Further Resources



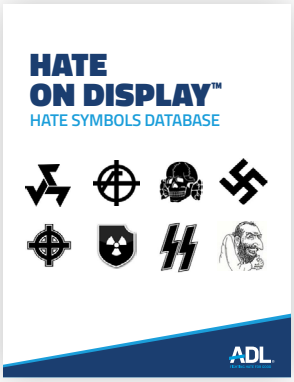
[ADL Law Enforcement Programs]



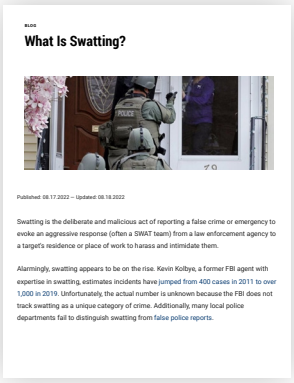
[ADL Center for Technology and Society]



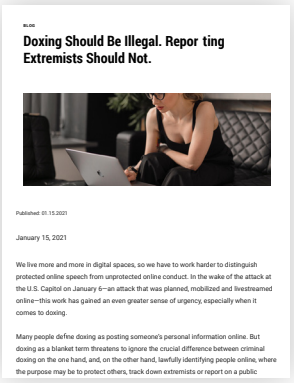
[ADL Center on Extremism]



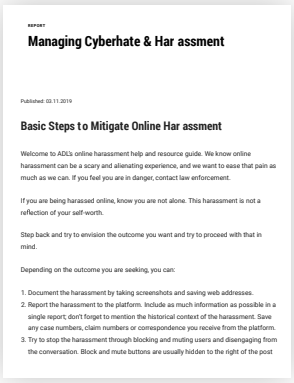
[ADL Hate Symbol Database]



[What Is Swatting?]



[Doxing Should Be Illegal. Reporting Extremists Should Not]



[Managing Cyberhate and Harassment]

ADL is a leading anti-hate organization. Founded in 1913 in response to an escalating climate of antisemitism and bigotry, its timeless mission is to protect the Jewish people and to secure justice and fair treatment to all. Today, ADL continues to fight all forms of hate with the same vigor and passion. ADL is the first call when acts of antisemitism occur. A global leader in exposing extremism, delivering anti-bias education and fighting hate online, ADL's ultimate goal is a world in which no group or individual suffers from bias, discrimination or hate.

Learn more at www.adl.org