INSI

Digital Defence

Managing Online Abuse Inside and Outside the Newsroom

JOURNALISM | SAFETY | RESPONSIBILITY | COMMUNITY

Contents

Introduction

The media industry is grappling with an unrelenting wave of online harassment targeting journalists—from state actors and organised crime networks to bots and members of the public emboldened by anonymity. Hate speech, disinformation, and threats of physical violence are a daily reality for many colleagues. Some are forced out of the profession; others endure long-term psychological harm—all at a time when independent, in-depth reporting is needed more than ever.

Digital violence is notoriously hard to contain. But what is clear is that journalists expect their employers to take charge before, during and after attacks—offering support but also concrete action.

INSI member organisations have been meeting since 2020 to share approaches and hard-earned lessons. The Google News Initiative and Facebook supported and participated in the early stages and we acknowledge their contributions.

This guide – written for INSI by Mike Christie, a key contributor to those efforts – is grounded in those conversations and all those that followed. As global head of safety at Reuters, he helped set the benchmark for how news organisations can protect their staff in the face of physical, digital, and emotional threats. His work has been instrumental in shaping industry-wide best practice.

The guide is designed to help newsroom leaders – across editorial, security and HR – create a practical framework to mitigate the impact of online abuse and be ready if digital threats escalate into real-world danger.

Every newsroom has a distinct risk profile, culture and resources. But they should not fight digital violence alone. Sector-wide collaboration – engaging with platforms on enforcement and accountability, and with governments on meaningful regulation – will generate greater impact than isolated efforts. INSI encourages all our members to actively participate in these shared initiatives, and to embed the spirit of collective resilience into their newsroom response.

We recognise that many newsrooms are already deeply familiar with the scale and nature of online abuse – and that time is in short supply. That's why this guide starts with the most urgent and actionable measures. It opens with a practical framework for responding to digital harassment, aimed specifically at managers responsible for staff safety and support, then turns to the broader context and background.

In the appendices, you'll find checklists covering key mitigation strategies including self-doxxing and response planning. We hope this guide is a useful and accessible resource for journalists, managers and safety professionals alike.

Preemptive countermeasures

In today's hyper-connected world, journalists face growing risks as attackers exploit cloud-linked devices and shared data across platforms. A vague threat is troubling—but when it includes a child's school name or a photo of a bedroom left online by a real estate site, the danger becomes far more real. Proactive planning is essential to keep newsrooms prepared.

1. Quantify the problem

Conduct a newsroom survey to understand how big the problem of online harassment and related abuse is for your news organisation. Be sure to canvas women and minority journalists as they suffer the most from online abuse.

2. Provide training

Include basic information about online harassment, its impacts and the company's response in all hostile environment training and information security courses. Special workshops focused solely on online harassment are another option.

3. Create reporting channels

Publicise the communications channels available to report online harassment, particularly those coming through personal messaging or social media. This could include a Teams or Slack channel, or simply an email address. Consider creating a channel for journalists to share their experiences of online harassment which might identify emerging trends and provide an opportunity for them to support each other.

Ensure the editorial safety team is aware in advance of reporting that could trigger an online campaign, rather than waiting to deal with the fallout.

4. Conduct self-doxxing

Ask journalists to run through basic self-doxxing exercises to see how much potentially sensitive information can be discovered online. It is impossible to eradicate everything accumulated over decades of online living – anyone who owns a property in the United States will have their address appear in public records, for instance. But information may be leaking through social media profiles whose privacy settings have not been properly locked down. Include this in the on-boarding process for new hires.

5. Take deep dives

Conduct deeper research into online vulnerabilities for high-profile journalists and those working on sensitive projects. Information security and risk management departments may be able to do this or hire an external vendor.

6. Use online deletion services

Send automated opt-out requests to data brokers which collect personal information about consumers and sell it using online deletion services such as DeleteMe. Though not available in all countries, subscribe to an enterprise-level service for the newsroom or get individual accounts. These services do not generally address the original source of the information being collated and sold but can help to limit its spread.

7. Employ threat monitoring services

Many media organisations subscribe to brand and reputation monitoring services that can detect copyright infringements, imposter websites or accounts, and critical commentary or reporting that might undermine a company's reputation. Similar services are available for monitoring security threats against a news organisation and online threats to individual journalists. Some scour the dark and deep web and less accessible areas such as chat groups on Telegram.

8. Delete old posts

Consider cleaning up public comments from more reckless, younger days if they could compromise a journalist's safety or integrity. Political opinions, even if no longer held, can disqualify journalists from covering election campaigns. Photos of hedonistic behaviour at college parties might become a safety problem if the journalist is dealing with ultra-conservative groups. Consider incorporating this into onboarding processes.

9. Keep profiles 'low detail'

A TV reporter's smiling face may be an important part of their brand, but does an investigative financial news reporter need to post a headshot on their profiles? Profile photographs could be used to track journalists via facial recognition software. Women journalists, who receive far more online abuse than men, could consider creating gender neutral online profiles.

10. Separate the personal and professional

Consider completely separating private and professional online personas, creating separate accounts. Private profiles should be limited to friends and family, be totally locked down and exclude sources and colleagues. Professional profiles should contain minimal personal information and be focused on work, developed with an understanding that any information might be public and could be used by an adversary.

11. Provide public appearance training

Provide training on how journalists should handle public appearances. Far-right groups often try to trap journalists into making embarrassing or damaging comments by asking them provocative questions in public then publishing their answers online. Others pretend to be sources offering concocted scoops with the aim of getting evidence of bias that can undermine a journalist's credibility.

12. Identify vulnerable people or groups

Some journalists may need additional training or support including:

- Political reporters and fact checkers
- In countries where online harassment has been weaponised by the state
- Women, people of colour, LGBTQ+ people
- Those with a high-profile online presence; who have been publicly criticised by personalities or leaders; and who have covered geopolitical flashpoints that have polarised public opinion

13. Moderate comments

Keeping online discourse safe and civil in the comments is a major challenge and requires dedicated resources. Some news organisations simply switch off comments. Others use automated tools or a combination of AI-driven automation and human moderation.

Hateful comments directed at a corporation and its website rather than at a specific journalist have less immediate impact but should nonetheless be monitored in case they express an intent to carry out harm in the physical world.

14. Establish a multi-department response team

Responding to severe online harassment may involve various departments. Get engagement in advance to ensure you have a comprehensive response ready. Set up a task force or working group to manage major incidents which includes:

- **Editorial management.** Decides on moving journalists to a safer location, hiring security or bringing in law enforcement.
- **Editorial safety.** Manages all threats to journalists' physical, emotional and digital welfare.
- **Information security.** Blocks attacks, identifies where they are coming from, determines their seriousness, logs incidents and analyses trends.
- **Corporate security.** Bars known harassers from the newsroom or premises.
- **Legal.** Takes legal action against online harassers and considers free-speech constraints.
- **HR.** Provides emotional support or counselling services to journalists coming under attack. Provides input on moving journalists out of a danger zone.
- **Communications.** Intervenes publicly as an institution about an online attack, for example in a comment thread.
- **Peer support.** Ensures affected journalists are supported by colleagues.

15. Provide editorial safety guidance

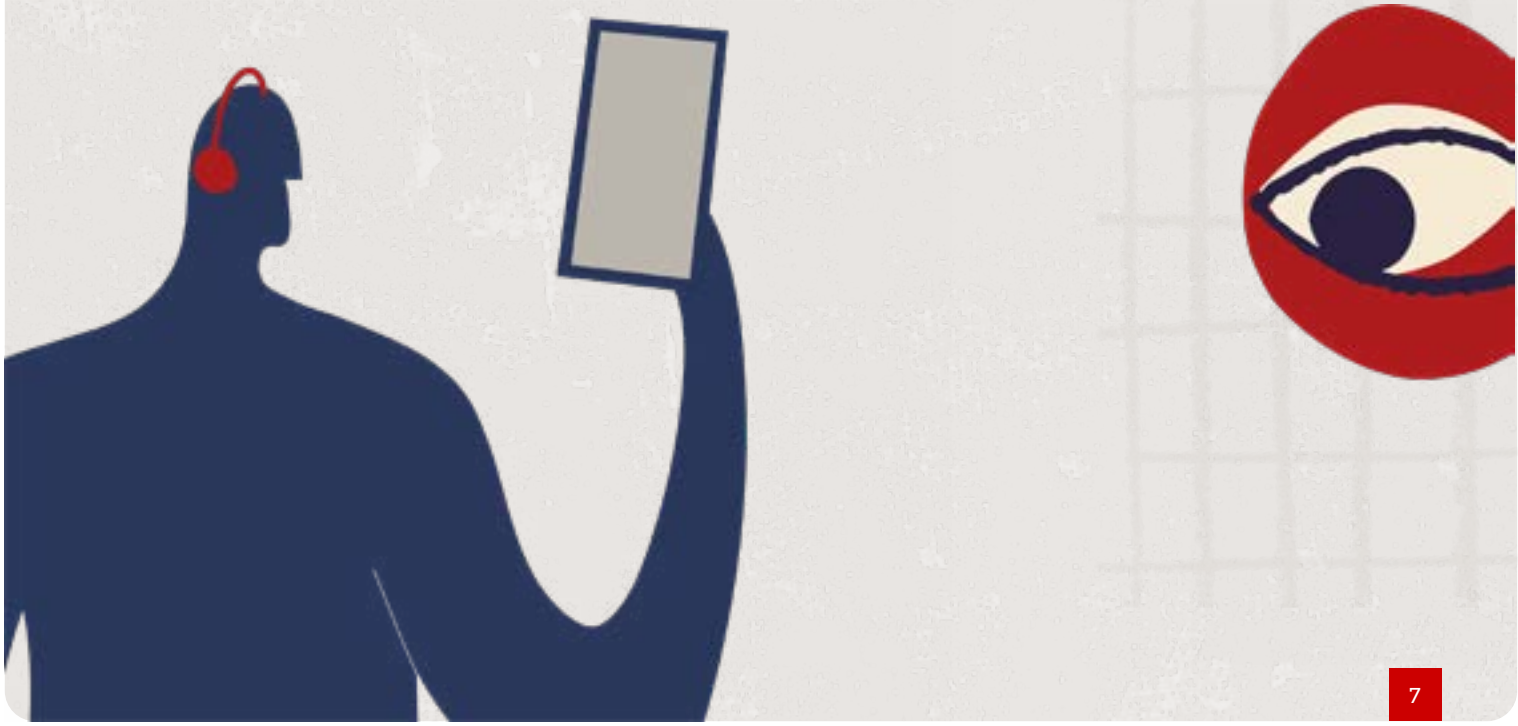
A news organisation's library of safety guidance should include material on the nature of online harassment, its effects and how the company supports journalists. Basic information security guidance should also include online harassment.

16. Reduce risk

BYOD (Bring Your Own Device) policies and the widespread use of freelance contributors makes it difficult to reduce the attack surface of newsrooms and journalists. A secure app used for chatting with a sensitive source might be on both a company and personal laptop. Chats may be backed up insecurely in the cloud to accounts which corporate information security cannot access.

There are ways to reduce the risks including:

- Consider publishing highly-controversial stories without bylines. This is often opposed by journalists, and their preferences should be considered.
- Review policies on publishing detailed reporter profiles on websites and linking to journalist's profiles in news stories. They may be popular with journalists keen to build their brands but also add to the amount of potentially sensitive personal information in the public domain. Most profiles will also contain photographs, allowing adversaries to track journalists through facial recognition software.
- The settings that enable content to be widely shared and go viral can also be used for harassment. Newsrooms could establish guidance on these settings and consider how they can be used safely and strategically.



Reporting mechanisms

Build trust with journalists

Online harassment does not always come through communications channels the company controls such as publicly visible posts or through emails, rather it is sent through direct messaging on personal social media accounts.

Journalists should report this abuse but often don't. They may think of it as a hazard of the job; believe it casts doubt on their integrity, professionalism, or the accuracy of their reporting, particularly if it calls into question their qualifications; or are concerned they will be taken off a story. Journalists need to be encouraged to report abuse. Ways to encourage reporting include:

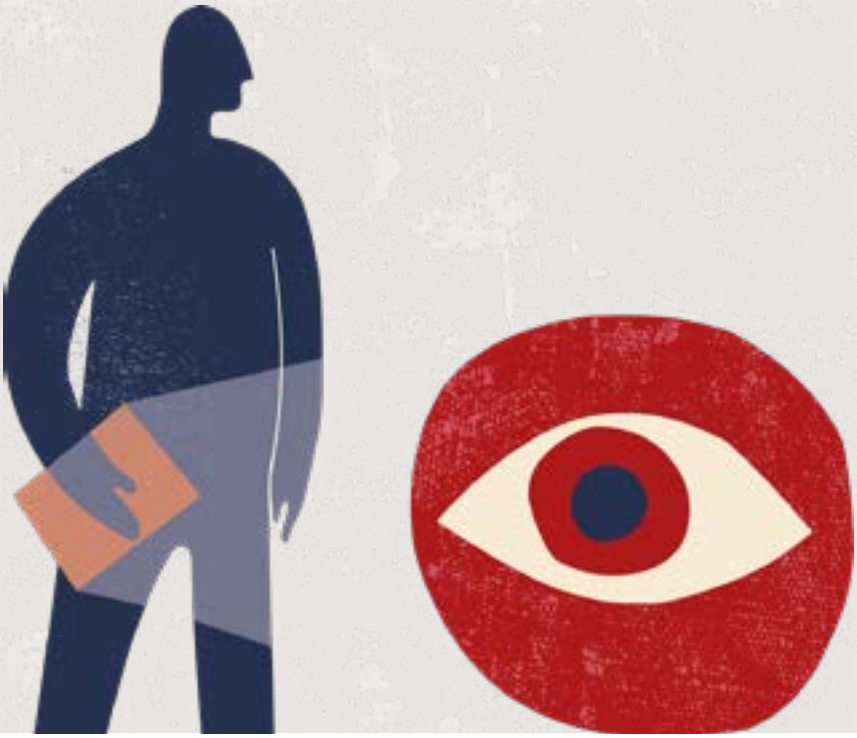
- **Training and awareness raising.** Journalists must not minimise the seriousness of online harassment. Training should outline how the company intends to stop the abuse, emphasise how it will support journalists and assure them they won't be taken off the story if they report it.
- **Create reporting channels.** Teams, Slack, Forms or email can be used. Monitor the reporting mechanisms or journalists will lose trust in the process.

Report abuse to the platforms

Some social media companies have established special partnership portals for reporting problems or designated liaisons. These portals will likely have a facility for reporting hijacked accounts, stolen credentials, online abuse and other problems. There may also be a designated liaison in the social media company that enterprise users can reach out to directly if a problem occurs.

In other cases, individual users themselves may have to report harassment or other problems directly to the social media platform.

Managers should understand which platforms are being used by their journalists, and how they handle complaints.



Monitoring mechanisms

Publicly-visible online harassment can be monitored by tools that allow news organisations to detect wider threats to their newsrooms and facilities. Many of these tools are geared toward brand protection. Some may scour the dark and deep web, and perhaps group chats on apps like Telegram, in addition to the public internet.

Some newer products can be used to monitor threats or attacks that are channelled through direct messaging but will require a journalist's consent to include their personal social media accounts in this type of monitoring.

Another option involves automated screening tools that seek to shield journalists (and other internet users) from the toxic impact of hate messages. These tools can be used to hide from sight messages with certain words or content.

This sort of content moderation can be beneficial to the extent that it protects targets from some of the emotional harm, but it could also prevent an organisation from noticing or detecting serious threats that require a response. There are some new AI-driven versions that both screen the recipient from nasty messages and review the messages to identify threats that need to be flagged.

Response mechanisms

Once they have established effective reporting and monitoring mechanisms, newsrooms may find themselves analysing hundreds of messages to determine if any could have serious consequences in the physical world. Triaging online harassment to sort out the truly serious abusers who have a track record of criminality or violence can be like looking for a needle in a haystack.

Consider the following when deciding how to respond:

1. Identifying attackers

Google is often a good place to start and may render some surprising results. Usernames or aliases are often used across multiple sites which may help to identify the sender. Online services like Social Catfish can be used to reverse search email addresses while PeekYou can search through usernames.

A media company's information security department may also have the capability to determine where IP addresses are located. Many online attackers will use VPNs to obscure their location and open fake, one-off accounts when one is shut down.

2. Threat analysis and triage

Indicators that an online threat could turn into physical violence include:

- **Involves a direct threat such as "I will kill you."** In contrast, an indirect threat such as "you should be executed for treason" may be seen as free speech rather than an intention to harm.
- **Puts a journalist at increased risk.** Has their home address been revealed? Would they be unsafe if their location was made public?
- **The attacker is disguising their identity.** This may show that they know their actions are wrong. Attackers who use their real names may counterintuitively be more of a threat because they might not understand that what they are doing is wrong.
- **Location.** Someone living close by may be more of a threat than a person who needs to fly halfway around the world to get to their target.
- **Criminal record or history of violence.** Does the attacker have connections with violent groups or a weapons permit?
- **Escalation.** Have the attacks travelled from one platform to another and increased in volume and stridency?

- **Organised.** Is the government or another entity involved in the attacks? Have they previously shown they are willing to use violence? Could the government also take legal action or detain a journalist?
- **Bots.** Look out for new accounts with no obvious history, or those that have been involved in similar campaigns.

3. Shielding targets

Blocking online attackers can be tempting to protect the emotional health of journalists. However, blocking could also provoke an escalation which wouldn't be visible. Attackers will often create new accounts and simply resume the harassment.

Alternatively, the editorial safety team or information security department could take over the monitoring of personal social media accounts. However, journalists may be reluctant to hand over passwords or allow access to messages from sensitive sources.

In this situation, a colleague or an editorial supervisor could monitor the messages, looping in safety and information security specialists if necessary.

4. Taking action

Newsrooms must take fast action if it is decided that online harassment could lead to serious harm. Options include:

- **Calling in law enforcement.** Direct threats should always be referred to the police or federal agencies. Journalists may need to make the report themselves.
- **Locking down** offices.
- **Adding known attackers to lists of people denied entry** to the company's offices and informing external vendors and landlords.
- **Ensuring the security of the journalist's home or temporary accommodation** by providing a home security system or subscription to a security service.
- **Moving the journalist and their family to a hotel with good security** while the threat is being assessed.
- **Engaging bodyguards** for high-profile talent.
- **Redirecting corporate email and blocking offending accounts** on personal email.
- **Deciding who should monitor incoming threats** on behalf of the journalist.
- **Reporting the offender to the platform.** Journalists themselves may have to file a complaint through a platform's self-reporting tools.
- **Taking legal action.**
- **Reaching out to journalistic counterparts** from other organisations who might have information to help evaluate the seriousness of the threat.
- **Coming out publicly to support the journalist** to shore up their resilience and morale.
- **Reporting on the harassment.** This could be a healthy way to focus attention on an attack, especially if it is part of a wider trend.

5. Supporting the journalist

Receiving a blizzard of harassment can have a profound emotional impact. Organisational support is crucial for resilience and helping the journalist to continue to report fearlessly. Consider support mechanisms including:

- **Offering peer support and counselling** within the organisation.
- **Making clear that the company does not blame the journalist** or their reporting and will support them in continuing to cover the story.
- **Providing assistance in reporting the harassment** to the social media channel or filing a police report.
- **Doing a deep dive on the affected journalist's online vulnerabilities** to make sure there is nothing that the attackers could continue to exploit.
- **Reviewing and upgrading the security of the journalist's home.** Decide whether to move the journalist and their family to a safer location.
- **Redirecting the abuser's heat towards the company.** Adding official statements to a comment chain, or putting out a statement.

6. Extreme cases

Some online harassment may escalate to the point where the physical safety of the entire newsroom is at risk. An organised and deliberate campaign by a popular political figure to rile up anger and hate could make it unsafe to do any reporting in public, at certain events, or in some regions. Safety teams need to be alert to this possibility, and willing to escalate individual cases of harassment to senior management.

7. Keep records and document learning

Every new case of online harassment might be different and there may be lessons you can learn about how to respond to future attacks. Keeping records will allow your organisation to identify emerging trends. This will be invaluable in persuading senior managers and finance directors to assign funding to combat the problem.

Checklist for newsroom managers

Pre-emptive countermeasures	Quantify the problem	Conduct staff survey
	Offer training and awareness raising	Include in basic safety courses for all journalists
	Establish communication channels	Teams, Slack, email
	Conduct self-doxxing	Include in onboarding and make available to newsroom through self-teaching module posted on internal network
	Carry out deep dives	Consider using an external vendor
	Employ data deletion services	Subscribe to a data deletion service for at-risk journalists
	Carry out threat monitoring	External vendors can scour dark and deep web and less accessible areas such as chat groups on Telegram
	Delete old posts	Include in onboarding process
	Create 'low detail' profiles	Include in onboarding process and safety training
	Create personal and professional personas	Discuss separating personal and professional profiles with journalists and editorial teams
	Monitor vulnerable groups or individuals	Conduct additional safety workshop for factcheck team, politics teams, possibly presented by an external vendor
	Offer public appearance training	Provide training on how journalists should handle public appearances
	Engage in comment moderation	External vendor could provide
	Set up multi-departmental response team	Include editorial management/safety/social media editor/legal/peer support
	Offer editorial safety guidance	Publish on internal network
	Carry out risk reduction	Remove photos from journalist profiles

Checklist for newsroom managers

Reporting mechanisms	Set up channel for journalists to communicate harassment	Consider Teams, Slack, email
	Use channels for reporting abuse to platforms	Options include partnership portals, direct contacts at platforms, individual reporting by journalists
Monitoring mechanisms	Monitor public threats	Enterprise agreement with vendor XYZ
	Monitor direct messages	Consider employing the same external vendor, if the journalist agrees
	Use software that shields journalists from hateful messages	This protects targets from some of the emotional harm but could also prevent detection of serious threats
	Moderate and monitor comment threads	Consider employing an external vendor
Response mechanisms	Develop method for identifying online attackers	Social Catfish can be used to reverse search email addresses. PeekYou can search through usernames
	Conduct threat analysis and triage	Conducted by the safety team, possibly supported by external vendor
	Shield targets	Ask editors and colleagues to monitor messages if necessary
	Act on severe threats	Review target journalist's security; inform building administration; liaise with law enforcement; assist journalists in reporting threat; liaise with platforms; decide on legal options; peers reach out to journalist targeted and any colleagues affected by the attack
	Offer support	Direct manager or peers may be best placed to support the affected journalist
	Keep records	Information security department may take the lead on this

Appendix 1. Defining online harassment

Online harassment and abuse can take many forms and aims to harass, intimidate or shut up journalists. It can cross over into the physical realm and to emotionally harm its targets in a way that can have far-reaching consequences.

As technology evolves and artificial intelligence becomes more sophisticated, we will confront new forms of online harassment through delivery channels we are barely aware of today. The platforms currently harbouring the most toxic bullying and abuse are unlikely to be the ones we are most worried about in years to come.

Taking a more defensive stance and using proactive strategies that build up resilience is more helpful than focusing on specific platforms or relying on them to deal with reports of abuse. Online harassment may also fall into the orbit of free speech debates, complicating law enforcement's ability to intervene and making social media companies reluctant to take responsibility for content moderation.

There are some other definitions of online harassment here: PEN America; Harvard T.H. Chan School of Public Health; Dart Center for Journalism & Trauma

Why it matters

Newsrooms need to protect their journalists from online harassment to:

- Ensure they can report the news freely, fearlessly and objectively.
- Protect them and their workplace from physical threats.
- Support their long-term mental health and emotional wellbeing.

One of the primary aims of online harassment is to silence journalists and scare them away from reporting on issues, or into leaving the profession altogether. It is often effective. A UNESCO survey of women journalists in 2020 reported that 30 percent had censored themselves on social media after being attacked online. Another poll by the International Women's Media Foundation (IWMF) found 40 percent of female journalists had stopped writing about issues they knew would generate attacks and one third had considered leaving the profession.

This makes online harassment a corrosive threat to freedom of expression, as well as an existential threat to journalists and newsrooms holding the powerful to account through quality journalism and fearless investigating. In all cases, online abuse has the potential to harm its victims psychologically and emotionally, leaving lingering mental scars.

In some cases, online attacks can spill over into physical violence and direct threats. The UNESCO survey found 20 percent of global respondents reported being attacked offline in the physical world in connection with the online violence they had experienced. In the Middle East, that proportion was even higher - more than half of the women journalists in the region who told the UNESCO survey they had been abused online had also been attacked physically.

Weaponisation of online harassment

Online harassment has been weaponised in many countries as a tool of censorship and oppression. Autocratic governments, extremist groups, political operators or powerful and unscrupulous individual actors have used it to mobilise online mobs against perceived opponents or critics. The impact of a thousand threatening or insulting messages is much greater than that of just a handful.

Women and minority journalists

Women, journalists from minority backgrounds and non-binary journalists receive a great deal more online abuse than white male colleagues, much of it misogynistic or racist. When a news organisation wants to find out the extent to which members of its newsroom are subject to online abuse, it should make sure to canvas its women, minority, and LGBTQ journalists as they are likely to be the main targets.

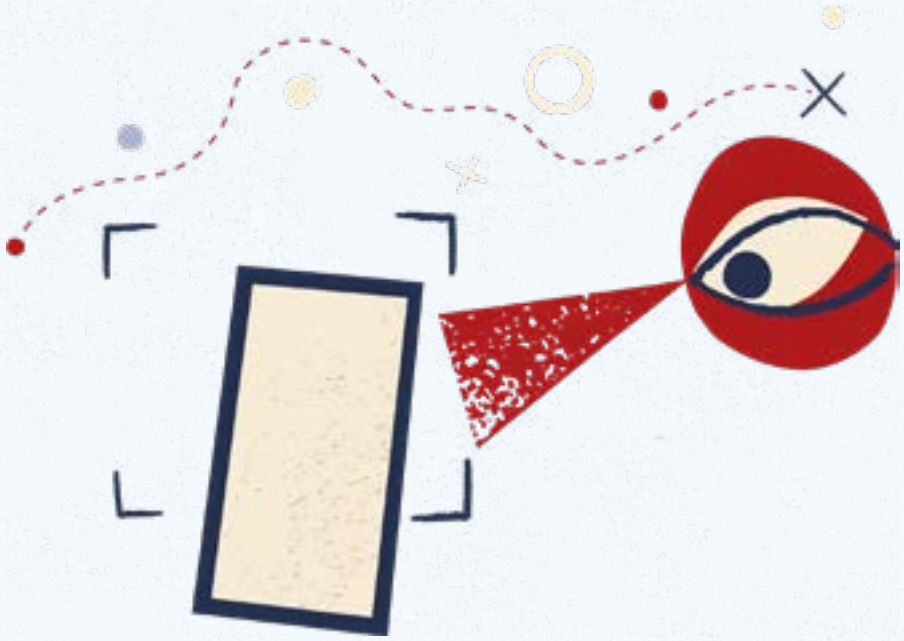
Topics attracting online hate

Political news in polarised countries such as the United States is a lightning rod for online attacks. Countries run by autocrats or illegitimate regimes may often suppress dissent and seek to weaponise online harassment as a tool to silence.

In areas where ethnic, tribal or sectarian rivalries have led to conflict, reporting deemed to be critical of one party or which uses language perceived as one-sided can attract a reaction. This is a common problem when stories are translated by editors outside of the local context who may not be sensitive to language nuances.

Online gaming, amateur and meme-driven investing and sports and pop music are topics where passions run high that generate surprising amounts of online abuse. Other real-world issues that often lead to toxic online spaces include:

- The far-right and far-left
- Misogyny
- Antisemitism
- Culture wars
- Disinformation
- Racism
- Debates over free speech versus censorship
- Geopolitical tensions



TYPES OF ONLINE ATTACKS

Threats of harm

Threatening to execute, bring to justice, rape, kill, hunt down or target family members including children. Some are direct threats which might warrant a law enforcement response but most skirt the edge of criminality or fall under the protection of free speech.

Cyber mob attacks/dogpiling

Encouraging others to target someone in a coordinated campaign. This might involve numerous harassers reporting a journalist's account for infringing the terms of service of a platform to get them removed. Governments, militaries or political parties may use semi-official troll farms to generate a mob attack.

Cyberstalking

Harassing and intimidating a victim over a long period. Stalkers may use surveillance, identity theft and other acts of cyberbullying. Cyberstalking is often a criminal offense and targeted journalists should get legal advice, as abusers may be mentally or emotionally unstable.

Doxxing

Releasing sensitive personal information such as a home address or the name of a child's school. Aggressors may publish this personal information to encourage others to harass, surveil, physically assault or steal the identity of a targeted journalist. Doxxing can occur while a journalist is on a high-risk assignment in a potentially dangerous location.

Online impersonation

Creating fake social media accounts to post derogatory or inflammatory messages intended to ruin their target's reputation or encourage wider harassment. Other objectives could include financial fraud or swaying public opinion.

Swatting

Making a false report about a crime such as murder or a hostage-taking in order to get police to raid a target's home. In the United States, police SWAT teams are heavily armed and expect to come under fire, so raids can be extremely dangerous and often result in fatalities.

Appendix 2. A guide for journalists dealing with digital violence

Online threats and harassment are designed to shut journalists up and make them self-censor. Receiving a flood of threats can be scary and have an emotional impact. Online attacks can also lead to physical violence.

Tell your supervisor or editor if you come under serious attack.

Increase your resilience to online harassment by minimising the amount of personal information available about you online. A general threat is bad enough but even worse if an attacker knows where your child goes to school or your home address.

Conduct a self-doxxing exercise and lock down the privacy settings on your social media accounts.

Consider creating separate public and private personas online, minimising the amount of personal information you share with the world through your professional accounts and keeping personal accounts just to family and friends.

Information security

Update your software and apps

Vulnerabilities are discovered all the time in the software that powers our computers and phones and which hackers and criminals rush to exploit. This applies equally to our phones, laptops and desktop computers. Look after your private computers and phones as well, and make sure all your software is up to date.

Never click on suspicious links

More than 75 percent of cyber-attacks take place through "phishing" emails containing a link or attachment which compromises your computer. If an email tells you something is really urgent, asks you to enter your account details, or has strange spellings, seek support from your IT department or use a programme like Dangerzone to open the attachment safely or in a sandbox environment.

Use a password manager

Off-the-shelf password cracking programmes can guess hundreds of millions of passwords per second and be loaded with information about a specific person from their social media accounts. Consider using a password manager like 1Password, Dashlane or KeePassXC to generate random passwords for every account and store them safely. Make sure your master password is tough to crack.

Check if you've been hacked

have i been pwned? shows which of your accounts have been compromised. Change the password of any that have been hacked.

Use two-factor authentication

Activate two-factor authentication. This sends a supplementary access code through text messages or via an app like Google Authenticator or Symantec's VIP Access. An app is preferable as SMS messages can be intercepted if your SIM card is cloned.

Regularly assess information security threats

You may not think there is anything sensitive about your story, but you cannot always predict whether it may lead to something sensitive that needs to be protected. Think about information security right from the start of an assignment and take the basic information security steps outlined in this document long before a routine story becomes highly sensitive and needs additional security measures.

Get a burner phone

Consider whether you should take your usual phone to meetings with sources if you are reporting on a sensitive story. Skilled trackers could use your phone to place you and the source at the same location, compromising their security. Talk to your supervisor, editor or IT about whether you should use a burner phone.

Connect with a VPN

Use a VPN – which encrypts your connection to the internet – when you connect your work and personal laptops and your phone to poorly-secured public Wi-Fi hotspots in hotels and airports. Proton VPN is a good free option.

Use an encrypted app for sensitive comms

WhatsApp, Signal or Wire are all good options though WhatsApp's owner Meta retains the so-called "metadata" – who you contacted and when – though not the substance of your chats. Telegram is not automatically encrypted unless you select the secret chat option.

Encrypt your hard drive

The hard drive on your laptop should be encrypted by default. If not, the information on your computer can be easily accessed. If it is encrypted and the computer is switched off, the information is secure. The same applies to phones.

Use secure versions of websites

Always make sure that websites you access are secure. Use the HTTPS Everywhere plugin to ensure that you use the secure version of websites. Avoid websites with only http:// rather than https:// at the beginning of their address.

Encrypt sensitive files and documents

VeraCrypt and 7-Zip are free, open-source encryption programmes for encrypting folders and files.

Avoid USB charging stations

Always charge your phone at a power socket rather than a public USB charging station. In Brazil during the 2014 World Cup, some of the USB charging points at Rio airport were installed by a criminal gang who were siphoning information off travellers' phones. Get a data blocker to ensure only power is getting through when plugging a USB cable into your phone from a public charging station.

Secure your devices

Keep your phones and laptops close to you when working on sensitive reports. If you leave a laptop in a hotel room, there is no way to know if someone accessed it while you were away.

Use apps that detect if your phone has been targeted by malware including iVerify which allows users to run a free deep scan once a month and F-Secure's Mobile Security app (formerly Lookout Lite). Malware installed in short-term memory can often be removed by rebooting your device.

Take extra care when crossing borders

Put sensitive information in Cloud storage before crossing borders. Sign out of accounts or apps in case a border official demands access to your phone or laptop. Power down your devices to make it difficult to access the information.

Dealing with doxxing

Information posted online can make us vulnerable to people who don't like our stories. Aggressors might look for past social media posts that undermine our credibility as journalists or reveal personal details like a home address. They might hope the information they post will incite others to attack us physically. Trolls may also try to dig up sensitive or compromising information to intimidate or punish them.

- They may "swat" you, by calling the police and reporting a fake hostage situation
- A feminist cultural critic who challenged the male domination of the gaming industry faced rape, bomb and death threats
- A troll can also become a real-life stalker

You may need to dox yourself (known as self-doxxing) to see what is available about you online that trolls could use. Consider taking the following steps:

Search Google

Searches on Google, Bing, Yandex, DuckDuckGo and Baidu. They each may uncover different results, especially if you have lived abroad.

"Firstname Lastname" OR "username"	Use quotes to search for an exact word or set of words. Search different combinations of your name, frequent usernames, and email addresses.
1."Firstname Lastname" - "Medianame"	1.This will exclude results that include your media organisation "Medianame", showing results otherwise buried in later pages. The minus sign is also a good way to remove results about other people who share your name.
2."Firstname Lastname" "Medianame" -site:Medianame.com	2. Search for pages that mention you and your media company, while filtering out pages from its website Medianame.com
"Firstname * Lastname"	The asterisk acts as a placeholder for any wildcard terms, for example your middle name or initial.
"(650) 656-5656" OR "6506565656"	Search for your phone number. Include alternate formats.
"username@gmail.com" filetype:pdf	This will show any PDFs listing your personal email, for example alumni publications or past presentations.
"Firstname * Lastname" 101 Main St Los Angeles CA	Search for associations to past addresses, cities, towns, institutions, jobs, publications ... things people know.
Firstname Lastname site:reddit.com	Search specific sites to find results not indexed by search engines

Do a reverse image search

- Use Yandex image search to search for photos of you. Upload an image of yourself using Yandex's reverse image lookup
- Upload your X, Facebook, LinkedIn and Instagram profile photos to TinEye to see where else they are being used

Lock down social media privacy settings

Social media platforms collect information about you to sell advertising. Control how they use this information and how much they collect by adjusting your privacy settings. Remember that privacy settings change and may need updating.

Facebook

Start with Facebook's privacy self-help tool:

- Type "Privacy Checkup" in the search field on the homepage and click "Visit."
- Review who can see your profile details. Make sure none are "Public."
- Limit who can see your posts to "Friends," "Specific Friends," or "Only Me."
- Remember your cover photo is always public. Replace it with one that does not show your face.

Take these additional steps in the "Activity Log":

- Click on "Use Activity Log" to review your timeline. Hide or delete anything you want hidden. Make sure there are no photos in "Photo Review". Photos will appear here if you have enabled face recognition which you can disable.
- Click on "Activity You're Tagged In" to see who has tagged you. Depending on the privacy settings of the person who made the post, this might be publicly visible.

Next

- Go back to the "Privacy" page and click on "Limit Last Posts".
- Review who can see the apps you use and how you can be discovered.
- Check the privacy settings of friends. Your comments or likes on their pages, and their comments and likes on yours, may be discoverable. Even if you're not tagged, the truly dedicated may look through people connected to you, such as family and co-workers, or people who have interacted with public parts of your Facebook page such as liking your cover or profile pictures.
- Make sure you are comfortable with your "Ads" settings.
- In "Profile and Tagging," enable the option to review posts you are tagged in before they appear in your timeline.
- Check how your profile appears to others via the "View As" feature.

Instagram

Create a professional Instagram account and completely lock down your personal/private account, limiting it to friends/family.

- Change your account to "Private Account" so only those you approve can see your posts.
- Deselect "Show Activity Status" in messages and story replies so no one can see when you are online.
- On the "Edit Profile" page, deselect the option to allow your account to be suggested on other profiles.
- Location permissions are controlled in the privacy and security settings on the app on your phone. Turn off location access, or limit it to when you want to share.
- Check your message and story options in the "Tags and Mentions," and "Comment" controls.

LinkedIn

As LinkedIn is a professional tool for networking it will be a public profile with a photo that is open for the world to see. However, intelligence agencies routinely create fake accounts, connect with you and then check out your networks. LinkedIn has also become a popular platform for scam artists advertising fake jobs, for example.

Options to secure your profile include:

- Under "Visibility of Your Profile & Network" in "Settings & Privacy," make sure you are comfortable with how widely you share your name, connections and region.
- Review who can see your connections. Limit this to you "Only You" if you have connected with sensitive sources.
- Select "Private Mode" so those whose profiles you view won't see.
- Limit who can see your email to "1st Degree Connections."

Then

- Select "No" under "Profile Visibility off LinkedIn" if you do not want your profile to appear on other partnered platforms.
- Manage who can discover your profile from your email address or phone number if they aren't connected to you.
- Under "Visibility of your LinkedIn activity" then "Followers," decide if you want everyone on LinkedIn to follow your public updates or just followers.

Also

- Be wary of having synced contacts if you have any sensitive sources, and consider removing all synced calendar items.
- Ensure you have not posted an old CV with a home address.
- Remove your high school.

X

X is one of the main platforms for online harassment against journalists and among the first places attackers might look for chinks in your privacy armour.

Take steps to lock down your profile including:

- Decide if you want to use a photo which could be used in facial recognition programmes to track you and how much you want to add to your bio.
- Avoid adding your birthday to your profile as well as your location which should also be unchecked in "Your Posts."
- In the "Privacy and Safety" menu, select "Protect Your Posts" in the "Audience, Media and Tagging" section to limit who can see your posts. Set "Photo Tagging" to off.
- Decide who can send you messages in the "Direct Messages" section.
- Decide whether people who have your email address or phone number can find you in "Discoverability."
- Take care when synching the contacts on your phone with X if they include sensitive sources.
- Turn off "Personalized Ads" in "Ads Preferences" in the "Data Sharing and Personalization" section.
- Deselect the option to personalise your experience in "Inferred Identity" or share your information with business partners in "Data Sharing With Business Partners."
- Decide if you want your content to be used to train X's AI, Grok.

Personal websites

If you have a personal website, the domain will be associated with an address, phone number, name and email. This is an easy way to get your contact information.

- Go to DomainTools and enter your website URL and see if your personal information is publicly available.
- Consider hiding it using a privacy protection service such as Who is Guard.
- Check your domain registrar to see what free or paid options they offer to obscure personal information.

Change passwords on hacked accounts

If you've been hacked, your username and password may have been sold and may be available on the dark web.

- have i been pwned? will tell you if your passwords and usernames have been compromised in data breaches. Change the password immediately and those on other accounts using the same username/password combination.
- Use password managers such as Keeper Security to create long random passwords or passphrases.
- Enable two-factor authentication. Use an authenticator app rather than SMS to receive the 2FA codes.
- Use an email address that is well-secured like Gmail protected with a YubiKey.
- Consider creating an uncompromised username based on a new email account you only use for a specific purpose, for example shopping portals.

Data brokers

There are dozens of data brokers that collect information and collate it into reports which they sell. You can opt-out but this can be difficult and may need to be repeated which is time-consuming.

- Sign up to an automatic opt-out service such as DeleteMe or Optery which will do the hard work.
- Use the Permission Slip app to send automatic opt-out requests. The paid version has greater functionality.

Appendix 3. Useful tools and tips for journalists and managers

Tool	What is it used for
Tall Poppy	Full package of online harassment mitiga-tion services, from training to incident re-sponse and concierge service for VIPs
PEN America	Training
Troll Busters	Training and consultancy
Theseus	Threat analysis
DeleteMe	Removal of personal information
Permission Slip app	Removal of personal information
Mark Monitor	Brand protection, domain management, impersonation protection
Proofpoint	Impersonation protection
ZeroFox	Dark web monitoring, impersonation protection
Elv.ai	Content moderation, threat monitoring
Memetica	Threat monitoring
Interfor	Social media monitoring, threat monitoring
Ontic	Threat analysis and investigations
Dataminr	Threat monitoring
JustDeleteMe	Delete old accounts
TweetDelete	Delete old X posts
tweeteraser	Delete old X posts
Google's PerspectiveAPI	Comment moderation

Other resources

- PEN America's Online Harassment Field Manual
- Zebra Crossing's easy to use digital safety checklist
- One-to-one safety consultations from the International Women's Media Foundation
- Reporters Without Border's Online Harassment of Journalists report

INSI

INTERNATIONAL
NEWS SAFETY
INSTITUTE

International News Safety Institute
C/O Thomson Reuters Foundation
5 Canada Square
Floor 8
Canary Wharf
London E14 5AQ

info@newssafety. org
www. newssafety. org
@INSInews