CPJ The Committee to Protect Journalists

Editors' checklist

Protecting staff and freelancers against online abuse

The following checklist allows editors and commissioners to understand how well-prepared journalists are when it comes to protecting themselves against online abuse.

For additional safety information, please see CPJ's safety guidance on protecting against online harassment, removing your personal data from the internet, and protecting against targeted online attacks.

Editors and journalists should also consult CPJ's digital safety kit for more information on digital security best practices.

As part of the risk assessment process, consider the following:

□ Does the journalist already have a history of being attacked online? If so, this likely means that he or she will be attacked again.

□ Does the story involve contacting people who are known to harass others online, for example members of online communities or certain political groups and their supporters?

□ Is the subject of the story likely to cause the journalist to be attacked online? Be aware that certain groups are more active online than others.

□ Is your journalist aware of the risks of online abuse related to the story they are covering?

□ Your journalists are more likely to be attacked online just after publication. Be aware that others in the newsroom, including those who are publicly affiliated with the news outlet, may also be attacked online as a result of the story.

□ Be aware that journalists and newsrooms are increasingly being targeted by sophisticated online smear campaigns. These campaigns often try to discredit an individual journalist or the outlet by linking them to an issue, a government, or an organization. For example, by stating that the media outlet receives money from foreign governments.

□ Online abuse can sometimes lead to physical threats. This risk is greater if the people attacking your reporter online live locally.

The Committee to Protect Journalists (CPJ) is a member of the Coalition Against Online Violence (CAOV), which has numerous resources for journalists and editors on how to deal with threats of digital harassment and abuse. See the CAOV's Online Violence Response Hub for more information.

Before assigning a story:

Managing personal data

□ Ask the journalist to review what personal data is available about them online. They should do this using all search engines and using the incognito or private window option in their browsers. The journalist should review photos, video, and comments under stories, as well as any content on websites. For more information on managing and removing your personal data, see CPJ's safety note.

□ Journalists should be encouraged to remove data that could be used to identify them, locate them, or contact them through a means they do not want, for example through their personal email address. This should include any information posted or shared by family members and friends.

□ Both the editor and the journalist should be aware that online abusers often target a journalist's family members. Journalists may wish to speak to family members about this.

□ If based in the U.S., journalists should be encouraged to sign up to a service, such as DeleteMe, that removes their personal data from data-broker sites.

Account security

□ Editors and journalists should be aware that online harassers often target a journalist's account and try to gain access.

□ The journalist should secure both their work and personal accounts with two-factor authentication (2FA).

□ The journalist should ensure they are using good password security to protect both their work and personal accounts.

□ Journalists should avoid using their personal email address or phone number when contacting sources that have a history of harassment and doxxing, for example members of the far right.

□ Ideally reporters should be given a work phone for contacting possible hostile sources.

Consider the following:

□ Does the newsroom have a protocol for dealing with online abuse, including steps for reporting online harassment?

□ Has the newsroom planned for a situation of doxxing?

□ What tech support will you be able to offer a journalist should their online accounts be hacked? Does that support extend to a journalist's personal online accounts?

□ What mental health and wellbeing support is available for a journalist targeted by online abuse?