PRACTICAL GUIDE FOR WOMEN JOURNALISTS ON HOW TO RESPOND TO ONLINE HARASSMENT

REUTERS/ Raheb Homavandi

In partnership with

unesco

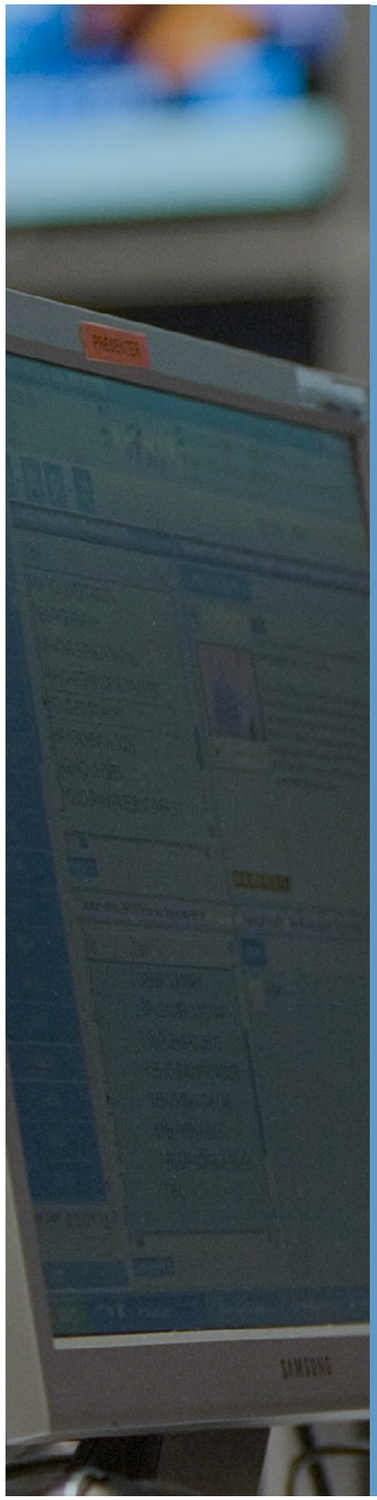
TrustLaw

THOMSON REUTERS FOUNDATION

With the support of

INTERNATIONAL WOMEN'S MEDIA FOUNDATION

CI-2021/FEJ/SOWJ/2



ABOUT THIS GUIDE

The publication of these guidelines was made possible thanks to the support of the Swedish Postcode Foundation. The content was developed by Ela Stapley (International Women's Media Foundation) under the coordination of the Thomson Reuters Foundation. Dechert LLP generously provided pro bono research. However, the contents of this report should not be taken to reflect the views of Dechert LLP or the lawyers who contributed.

UNESCO editorial coordination: Saorla McCabe, Theresa Chorbacher

Project support: Johann Bihr, Sara Bonyadi, Annina Claesson

Graphic design: Paula Figueroa

This resource is offered for information purposes only. It is not legal advice. Readers are urged to seek advice from qualified legal counsel in relation to their specific circumstances. The authors and contributors intend the report's contents to be correct and up to date at the time of publication, but they do not guarantee their accuracy or completeness, particularly as circumstances may change after publication. Neither UNESCO nor the authors and contributors accept any liability or responsibility for actions taken or not taken or any losses arising from reliance on this report or any inaccuracies herein. In accordance with the Thomson Reuters Trust Principles of independence and freedom from bias, the Thomson Reuters Foundation does not take a position on the contents of, or views expressed in, this resource.

INTRODUCTION

REUTERS/ Carlos Garcia Rawlins

"This online violence has serious implications for press freedom such as the restriction of women journalists' voices online"

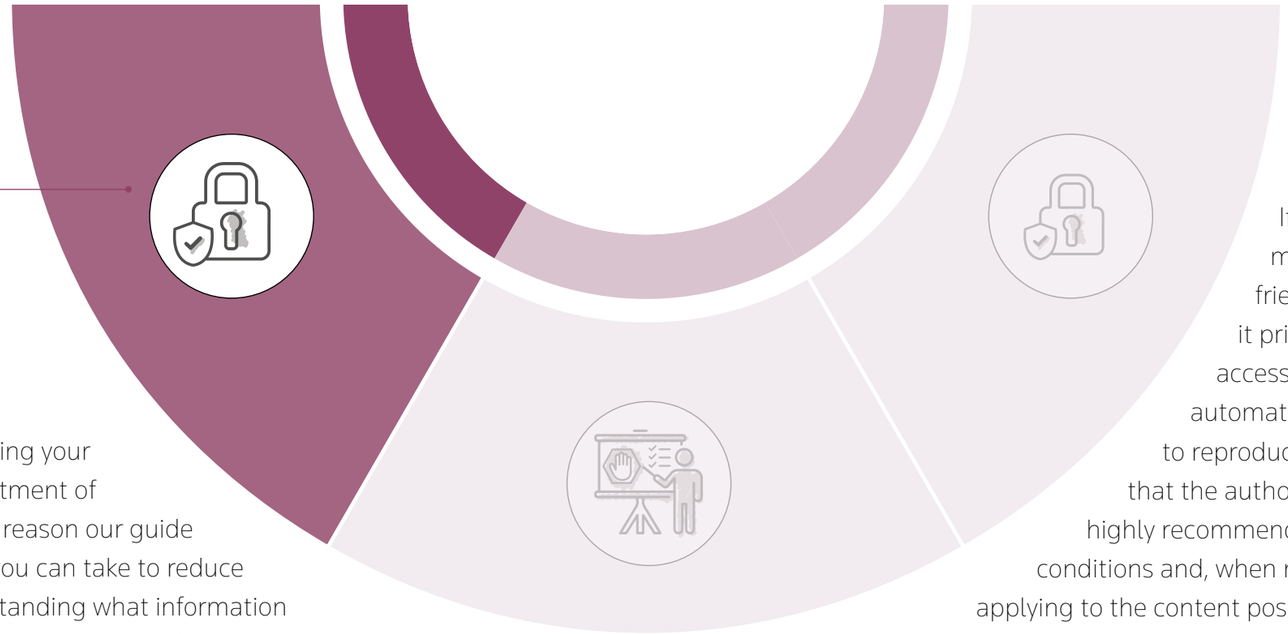
The growth of social media has seen journalists engaging in a digital public space as part of their role. This has created new opportunities for journalists, including women journalists, such as wider outreach, possibilities to connect with journalists internationally and possibilities to create specialized outlets. At the same time, this online presence also brings a number of risks. It has led to women journalists sharing, sometimes without realising it, personal information about themselves. This data is now being used against them. Online abusers scour the internet for information that can be used to intimidate and harass media workers and to stop them from doing their job. This is not the only concern, journalists frequently receive death threats, threats of sexual violence, threats directed at their families and are targeted by disinformation campaigns. Research has shown that these attacks disproportionately affect women journalists.

A 2020 survey of 714 women-identifying journalists from 125 countries, conducted by UNESCO and the International Center for Journalists (ICFJ), found that 73% had experienced online violence in the course of their work. According to the survey, women journalists affected by other types of discrimination such as racism and homophobia were even more likely to be targeted, and with more severe impacts.

This online violence has serious implications for press freedom such as the restriction of women journalists' voices online. While online platforms endeavour to prevent online attacks and States endeavour to prosecute the perpetrators, there are steps that journalists can take to better protect themselves and their staff. This guide has been written to support women journalists as they navigate the challenges of online violence.

01 PREPARING FOR ONLINE HARASSMENT

Taking steps to prepare yourself and your colleagues for online harassment is an important part of minimising risk. The more you can do in advance, the better protected you will be if an attack happens.



MANAGING ONLINE CONTENT

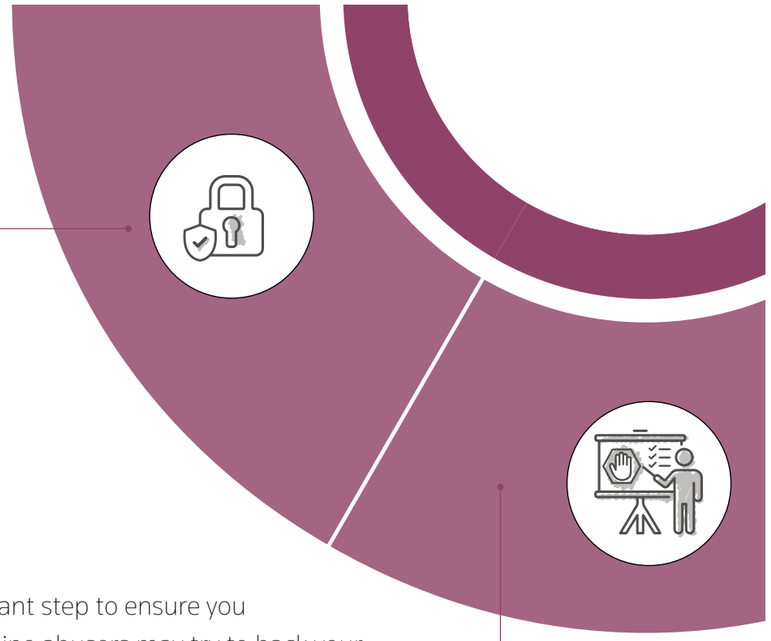
Managing your content online and protecting your data can be daunting - it requires an investment of time and necessary IT knowledge. For this reason our guide aims to lead you through some key steps you can take to reduce risks for yourself and your sources. Understanding what information is fine to share and what data is best kept private is key to better protecting yourself. Information that can be used to verify your identity, contact, or locate you is best kept offline. This includes data such as your date of birth, your personal phone number, and your address. Carrying out a mapping of your online data and where it is stored is an important first step. The International Women's Media Foundation (IWMF) course Keep it Private gives a more detailed insight into personal data and how to protect it.

Search for your name online using all search engines and ensure you review videos and photos as well as websites. Online attackers will often target women journalists by looking for photos of them at the beach or gym which they then circulate on the internet accompanied by abuse and threats which are misogynistic in tone. Keep a note of any content that you are uncomfortable having online. Next, start to remove the content.

If the information is stored on your social media sites or on the sites of family and friends, then you should delete it or make it private. It should be kept in mind that the access settings of some social networks are automatically set so that third parties are allowed to reproduce any content posted online, assuming that the authors gave their prior consent. Therefore, it is highly recommended to always verify the legal terms and conditions and, when necessary, to modify the access settings applying to the content posted on social network accounts. Be aware that copies of that data may still exist somewhere else on the internet, such as internet archive sites like the Wayback Machine.

Managing your online content is crucial as your data may end up on a third-party site, such as a public database or a social network, and it can be difficult to get the information removed. This may indeed require obtaining a court judgment ordering either the site or the access provider to remove the personal information or the whole page displaying it. Journalists should research their rights with regards to getting their data removed from public databases as this often depends on the law of the country they are living and working in. The Committee to Protect Journalists has a more detailed guide on how to remove data from the internet.

01 PREPARING FOR ONLINE HARASSMENT



ACCOUNT SECURITY

Securing your online accounts is an important step to ensure you are better protected against harassers. Online abusers may try to hack your accounts, take them over and post content that could be harmful to you professionally. They may also be looking for data, such as photos or videos, that they can use to discredit you or blackmail you and your sources. To secure your accounts, ensure that you are using a password manager and creating long passwords of more than 16 characters in length. You should not reuse passwords because if an online attacker gets access to your password, they will be able to log into more than one account. You should also ensure that you turn on two-factor authentication (2FA) for all your accounts. This is an extra layer of security that will reduce the risk of someone accessing your accounts. To find out more about account security, the Rory Peck Trust has a detailed guide.

REUTERS/ Anushree Fadnavis

THINK ABOUT WHO MIGHT TARGET YOU AND WHY

There are many different types of online attackers and they use different strategies to target journalists. Understanding who may wish to target you and why can help you better prepare. Before publishing a story, it can be helpful to try and predict any online backlash and the form it will take. This will help you mentally prepare for online harassment as well as put in place any strategies for dealing with it. It can be helpful to map out different kinds of groups that engage in online hostility and the strategies they tend to use. Newsrooms are encouraged to build in preparation for online abuse as part of a risk assessment process. PEN America's Online Harassment Field Manual has a guide to online attacker strategies and the IWMF has a detailed Know your Trolls course, for journalists looking to learn more about who online attackers are and why they attack.

01 PREPARING FOR ONLINE HARASSMENT

DOXXING

Doxxing is an increasingly common tactic being used against journalists as a way to intimidate them, which consists of collecting and disclosing personal details online, such as a home address, or private contact details, with a call out to internet users to use the data to harass or harm the victim, whether online or in real life. If your location is posted online and is being circulated with threats being made against you, then you are at risk of a physical attack. Newsrooms should plan for doxxing and have steps in place to protect journalists who have been doxxed because of their work. This should include discussing the possibility of doxxing in risk assessments and, if possible, having a plan for emergency relocation. Journalists should ensure they speak to their editors if they are concerned that a story brings with it a risk of doxxing. Freelance journalists should discuss threats of doxxing with colleagues, journalist networks, as well as their commissioning editors who may be able to support them in case of an incident. The New York Times has a detailed guide on how to better protect yourself against doxxing. Depending on the jurisdiction in which it took place, doxxing may be prosecuted under the legal provisions relating to violation of privacy or harassment.

IMAGE MISREPRESENTATION

Online attackers often look for online images of women journalists that they can use to discredit them or cause them harm. This strategy of online attack involves taking an image and portraying it out of context, often with a sexual connotation. Attackers may also doctor images, superimposing the woman's face onto pornographic material. Online attackers will often find photos or videos from a journalist's social media sites, so it is important that journalists review what images are publicly available. Some videos and photos may have been published with their (implied) consent, for instance when they were taken in the course of their public professional activity, i.e. during an interview or a coverage, or for an article. Journalists should take steps to either remove or limit access to any photos or videos they feel could be used to target them. Online abusers may also hack accounts or devices looking for images that they can use to blackmail women journalists. Journalists should follow best practice around securing online accounts (see page 5). Journalists may be able to take legal action against any use and/or representation of their image which is not related to their public professional activity, and/or any distorted image in which they may be easily identified, if the content is published without their prior consent and could cause them harm.

02

SPEAKING WITH OTHERS

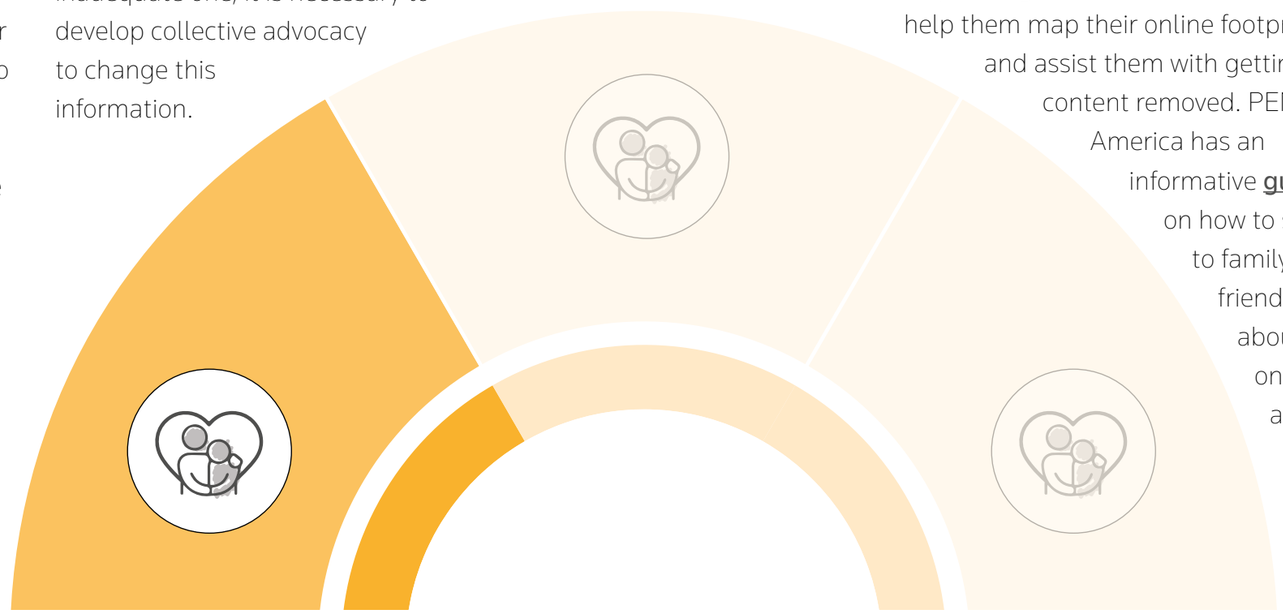
It can be important to speak with others about online abuse and its consequences. Letting others know what is happening to you can help you better protect yourself and your loved ones.

SPEAKING WITH YOUR NEWSROOM AND COLLEAGUES

If you feel able, you should speak with your editor or newsroom manager about online harassment. It can be helpful to think in advance of how your media outlet can support you and what you would like to happen. For more advice, PEN America has a guide on how to speak to employers about online abuse. Speaking to colleagues about your abuse can also be helpful. Setting up peer-support networks and sharing strategies for dealing with online harassment is useful, especially for freelancers and younger members of staff who may not feel so comfortable reaching out for help. It may be helpful for women journalists to join support groups both in and outside the workplace. These can provide much needed support when it comes to dealing with online abuse. Newsroom should encourage peer-support networks, create internal reporting mechanisms through which employees can safely and privately report online abuse, and have a plan in place to support journalists who are facing online abuse. This can include strategies for responding to online abuse, a plan for cases of doxxing, and providing trauma support for those who need it. PEN America has this informative guide for employers on how to support employees facing online harassment. UNESCO and the Thomson Reuters Foundation have also recently developed "Gender-sensitive safety policies for newsrooms" that could be useful in that context. If your newsroom does not have a policy on safety, or has an inadequate one, it is necessary to develop collective advocacy to change this information.

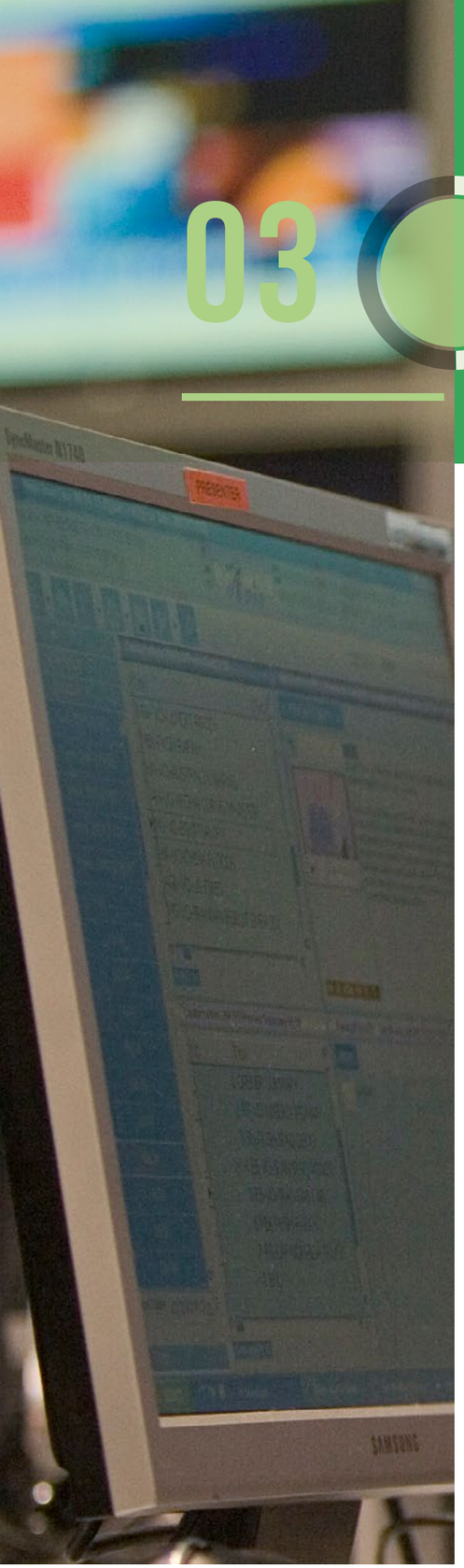
SPEAKING WITH FAMILY AND FRIENDS

Online abusers may also target family members and close friends, so it can be important to speak to them about harassment and how it can affect both them and you. Explain to them the importance of online privacy and let them know what content you are unhappy about being shared on the internet. Family members may not have secured their own online information so it can be helpful to work with them to remove data and turn on security settings. It can also be useful to help them map their online footprint and assist them with getting content removed. PEN America has an informative guide on how to speak to family and friends about online abuse.



PSYCHOSOCIAL SUPPORT

Online harassment has offline consequences for those who are targeted. Journalists who experience abuse often report feeling afraid, isolated and overwhelmed. The 2020 UNESCO/ICFJ survey found that 26 percent of targeted women journalists that participated in a survey stated online abuse had caused them mental health issues with 12 percent seeking medical assistance. It can help to seek professional support. Ideally, newsrooms should provide psychosocial support for journalists. Journalists who do not have access to professional help may find speaking with friends and colleagues beneficial. The Committee to Protect Journalists has this guide with links to resources that can help. The Dart Centre has a comprehensive overview on online harassment with guidance on responding to abuse.



03

WHAT TO DO DURING AND AFTER AN ATTACK

If you are targeted by a sustained online attack it can be difficult to know how to protect yourself.

FIRST STEPS

Journalists who have not taken preventative measures should review the preparing for online harassment section at the beginning of this guide. All journalists should review their accounts and ensure they are using secure passwords and have 2FA turned on. Media workers should speak with their editors about the abuse and the newsroom should provide support per their online harassment guidelines. For some journalists, it can be helpful to go offline and let a colleague or trusted friend monitor their accounts until the harassment has died down. Getting online support from other journalists or communities by asking them to tweet messages of support can also be helpful. It is also important to document any messages that cause concern. Details on how to document harassment can be found in the final section of this guide.

RESPONDING TO ABUSE

Knowing when and how to respond to online abuse can be a challenge. This is because there are many types of online abusers and identifying the motive for the harassment can be difficult. Responding to online harassers can make the abuse worse; however, there may be times when a response can be helpful. Journalists who are targeted by coordinated disinformation campaigns questioning the integrity of their reporting may benefit from pinning a response to the top of their social media feed. Ideally, they should do this with the support of the media outlet. Newsrooms are advised to create a policy around responding to online abuse and to share it with staff. Organizations, such as HeartMob and TrollBusters, also offer advice and support on responding to abuse.

DOCUMENTING AND REPORTING AN ATTACK

It is not possible to document all online abuse, but you may wish to document particular messages to show editors, pass on to the authorities, or to share with press freedom organisations. Journalists should consider documenting threats from repeat offenders, especially if they use their real name, as well as messages that contain death or rape threats. If possible, report abuse on social media platforms via dedicated report channels. Journalists should ensure they take screenshots of as many of the messages as possible, including the content, date, time, and the name of the harasser. It is advisable to create a spreadsheet to track the abuse with the date and time of the harassment as well as the platform you received the abuse on. PEN America has more details on documenting harassment here.

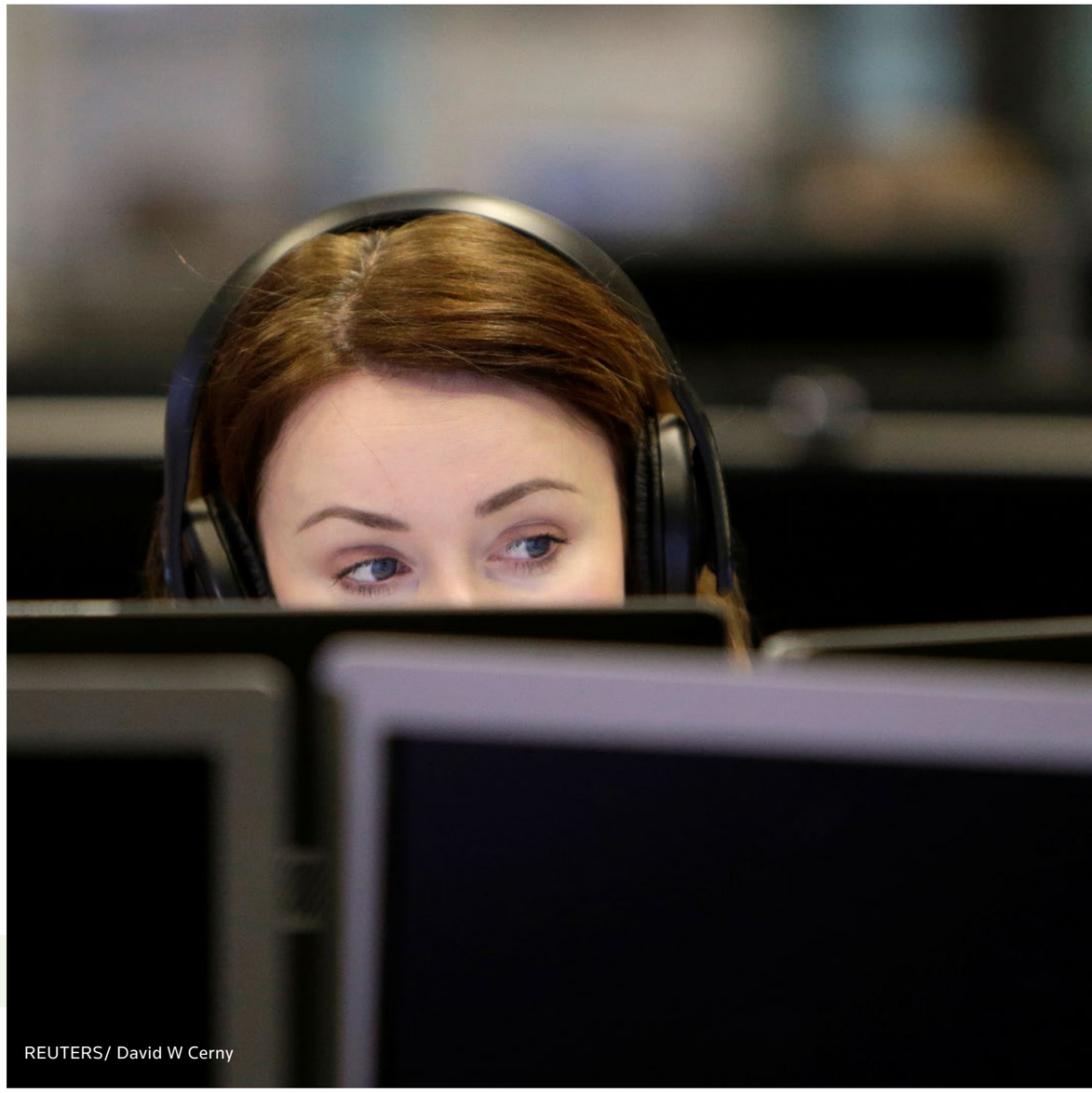
03 WHAT TO DO DURING AND AFTER AN ATTACK

PROSECUTING THE PERPETRATOR(S) AND SEEKING REMEDIES

Online harassment of women journalists may be prosecuted under various legal provisions, ranging from harassment and threats to provisions protecting freedom of the press. Depending on the jurisdiction, sexism or gender-motivated behavior may be considered an aggravating circumstance when these have motivated the commission of a crime or offence.

In practice, when faced with online harassment, women journalists may take various measures to stop or avoid further attacks, and to build up a case in view of a legal action including:

- First, especially in case of online impersonation and/or doxxing, liaising with sources and contacts in order to enable them to anticipate further harassment and to protect themselves;
- Second, collecting evidence such as testimonies and screenshots of messages and images received or posted online;
- Third, contacting the websites or platforms hosting the pages concerned to ask for the removal of the information and possibly demanding greater action in filtering out attacks and deplatforming attackers;
- Then, reporting the attack using the mechanisms set up by the local authorities, and, where appropriate, filing a complaint with the local police, with the assistance of a legal counsel if necessary;
- Consider the pro's and con's of reporting the abuse as a news or feature story to raise the issue on the public agenda


REUTERS/ David W Cerny

04 ORGANISATIONS AND RESOURCES

There are many organisations that have produced useful resources to support women journalists with responding to online harassment.

01	Access Now	Digital safety support available in English, Spanish, French, German, Portuguese, Russian, Arabic, Filipino and Italian
02	Dart Center	A Self-Defence Guide for dealing with the psychosocial impact of online harassment
03	Electronic Frontier Foundation	Surveillance Self Defense Basic Guides available in English, Spanish, French, Arabic and Portuguese
04	Digital Rights Foundation (DRF)	The DRF conducts research and trainings on online safety.
05	Frontline Defenders and Tactical Tech Security in a Box	General digital safety kit available in English, Spanish, French, Arabic and Portuguese
06	HeartMob	Online support and resources
07	Online SOS	Online harassment resources for a US audience
08	PEN America	Detailed guide to managing online harassment available in English and Spanish
09	SMEX	Guide on how women can protect themselves online in Arabic and English.
10	Tactical Tech	A manual including information on self-doxxing in Spanish
11	The Committee to Protect Journalists	Individual digital security assistance and resources available in a range of languages
12	The Committee to Protect Journalists	Remove personal data from the internet in English, Spanish and French
13	The Committee to Protect Journalists	Protecting against targeted online attacks in English, Spanish and French
14	The International Women's Media Foundation	Online violence program in English, French and Spanish offering individual digital security assistance for women journalists and resources to combat online harassment.
15	The International Women's Media Foundation and Free Press Unlimited	Know your Trolls available in English, Spanish, French and Arabic
16	The International Women's Media Foundation and the International Center for Journalists	Online Violence Response Hub
17	The International Women's Media Foundation and Free Press Unlimited	Keep it Private available in English, Spanish, French and Arabic
18	The International Women's Media Foundation and the Knight Centre for Journalism in the Americas	Online harassment: Strategies for Journalists' Defense
19	The NYT Open team	Self-doxxing guide
20	The Rory Peck Trust	The Digital Security Guide includes guides to online harassment and trolling (available in a range of languages).
21	Troll Busters	Resources for dealing with online harassment available in a range of languages
22	UNESCO	The UNESCO discussion paper is available here. Further resources, tools and research by UNESCO and partners can be accessed here.

REUTERS/ Damir Sagolj

Published in 2021 by the United Nations Educational, Scientific and Cultural Organization, 7, place de Fontenoy, 75352 Paris 07 SP, France. ©UNESCO

This document is available in Open Access under the Attribution ShareAlike 3.0 IGO (CC-BY-SA 3.0 IGO) License (http://creativecommons.org/licenses/by-sa/3.0/igo/). By using the content of this publication, the users accept to be bound by the terms of use of the UNESCO Open Access Repository (http://en.unesco.org/open-access/terms-use-ccbysa-en).

The designations employed and the presentation of material throughout this publication do not imply the expression of any opinion whatsoever on the part of UNESCO concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views and opinions expressed in this document are those of the authors and should not be attributed to UNESCO.

In partnership with

With the support of

With the support of