

Guidelines for Ukrainian newsrooms

STEPS FOR NEWSROOM TO TAKE IN THE FIRST 24 HOURS FOLLOWING AN ONLINE ATTACK AGAINST A WOMAN JOURNALIST



An online attack may have a detrimental impact on a journalist's mental wellbeing, physical safety, professional reputation, and willingness to continue her work.

The newsroom's actions in the first 24 hours are critical to stabilize the situation, prevent escalation, and rebuild confidence.

Why is this guide focused on women journalists?

This document focuses on responding to online attacks against women journalists, as numerous international studies (including UNESCO's *The Chilling*) prove that women in the media are disproportionately more likely to experience gender-based online violence — manifestations that demean their appearance, emotionality, sexualize them, and undermine their professionalism.

This is not to be construed as a claim that male journalists do not face online attacks. However, the nature, intensity and consequences of violence against women can have a deeper psychological impact and intersect with other forms of discrimination — based on age, region, ethnicity, etc.

! *We urge newsrooms to develop comprehensive policies for responding to online violence that take into account the gender-specific nature of the threats.*

1 Recognize the attack and support the journalist

- Contact your colleague immediately, either verbally or in writing. Confirm that you are aware of the situation and that she is not alone.
- Ask what kind of support she needs right now — psychological, legal, technical, or personal.
- Avoid evaluative statements like *“it’s not that serious”* or *“you brought it on yourself”* or *“that’s the nature of our job.”* Do better: *“We see what’s happened. It’s not your fault. We are there for you and we’ll help you handle this.”*
- Don’t shift the responsibility for the response on the journalist.
Online violence is a systemic problem rather than a personal matter.



2 Assess the level of the threat

Check if the attack contains the following:

Doxxing > publishing or threatening to disclose personal data (address, phone number, photos of family members, including children).

Threats of sexual or physical violence > *“You better not leave the house,” “You won’t live to see tomorrow,” “After the victory, journawhores will be lynched.”*

Coordinated attacks > repeated messages from different accounts.

Physical harassment > suspicious calls, surveillance.

Gendered disinformation > spreading fakes about alleged sexual relationships, affiliation with escort services, or personal profiles on porn websites.

Defamation > accusations of working “for grants,” “for the enemy,” for the authorities or a foreign government, for example, *“stupid order-taker,” “Soros’ leech”* etc.

Sexist and misogynistic insults > *“journawhore,” “why can’t she sit at home and raise kids instead of sticking her mug into politics. Such hags always have problems because they have a mic instead of a man”* etc.

Impersonation > creation of fake profiles, hacking accounts.

Revenge porn > threats to publish intimate photos or AI-generated videos.

If you check at least one item on the list, the risk is high. Contact the cyberpolice, a lawyer, and a psychologist.

3 Provide basic cyber protection

- › Check the passwords: change them to more complex ones if in doubt.
- › Activate two-factor authentication (2FA) for the email, social networks, and instant messengers.
- › Install a VPN and an antivirus.
- › If necessary, approach digital security specialists.

Who can help?

Nadiyno.org is a digital security hotline (created by eQualitie Canada): assessment of the organization's cyber risks, security settings, access management, creation and protection of logins, training for employees on the basics of cybersecurity, consultations on protection of local networks, and more.

Access Now is 24/7 technical assistance with digital security (also available in Ukrainian): rapid response to incidents, personalized recommendations, guidelines and further digital security support, assistance with risk assessment and developing security strategies of the organization or community, support with the protection of tech infrastructure, websites and social media against attacks etc.

Digital Security Lab – consulting, checking devices, account restoration, trainings for newsrooms: they check gadgets for spyware, restore access to online accounts, analyze phishing messages, set up the protection of online services against hacking etc.

4 Provide access to psychological support

- › Ask if the journalist wants to change the format of her work or take a pause. Support this decision and **do not perceive it as a weakness**.
- › If you have agreements with psychologists in place, refer her immediately. If not, help her find a professional.

Available opportunities:

Women in Media NGO – group and individual counseling:
ngo.womeninmedia@gmail.com

Support4Media – a psychological support program for journalists.

RSF (Reporters Without Borders) – up to 10 free sessions, on-site or online: assistance2@rsf.org

People in Need – 24/7 toll-free hotline: 0 800 210 160

5 Document the attack

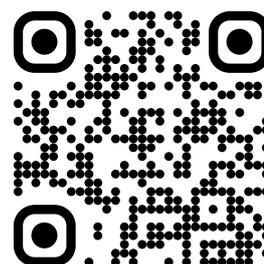
- › **Collect evidence:** screenshots, links etc., record the time of the attack and the accounts that participated in it.
- › Do this either together with the journalist or with her consent but **without coercion**.

This is important for:

- reporting the incident to the police;
- legal assessment;
- further internal or public response.

Women in Media NGO has launched an interactive map to document online attacks against Ukrainian women journalists. If you have experienced or witnessed such violence, report it. Your experience will help identify threats and strengthen the protection of women media workers.

Scan the QR code to view [the map of online attacks against women journalists](#) →



6 Engage a media lawyer (if available)

- › Check whether the threats are subject to criminal/administrative liability.
- › Seek advice whether it makes sense to report the incident officially to law enforcement or the media regulator.
- › If necessary, the editorial team should also file a statement in addition to the journalist's personal statement.

Where to get help:

Women in Media NGO

Get legal or other support by writing to:
ngo.womeninmedia@gmail.com

Human Rights Platform

Get legal advice: **info@ppl.org.ua**
or apply via website:
<https://ppl.org.ua>

Regional Press Development Institute (RPDI)

For individual legal assistance, please contact Head of RPDI Legal Department Oksana Maksymeniuk:
oksana.maksymeniuk@gmail.com

Hotline of the Institute of Mass Information (IMI)

Contact the IMI hotline for immediate assistance:
(050) 447-70-63

7 Determine whether to respond publicly

A public statement can:

- › protect reputation;
- › stop the wave of hatred;
- › show solidarity.

But it must be discussed with the affected journalist considering her emotional state and risks.

Detector Media NGO:

to disseminate a public statement or draw attention to a case of pressure, approach this media organization which focuses on freedom of speech and journalists' safety: info@detector.media

8 Inform the entire editorial team of the response policy

- › Even a short email, such as *"We know what happened, we are supporting our colleague, here is what steps we are taking,"* is important.
- › Show that an attack on one is an attack on the entire team.
- › Care should be taken to ensure that the policy on the use of social media should be reciprocal and also oblige the editorial team to support the journalist.

Additionally: Actions to avoid

- ✗ Do not downplay the threat (*“Oh, it’s just bots/trolls,” “We’re used to this,” “During the war, there are other more serious problems,” “But you weren’t physically attacked.”*)
- ✗ Do not force the affected journalist to make a public comment or to write a report on the incident.
- ✗ Give the affected journalist an opportunity to respond, keeping in mind that “don’t feed the trolls” is not an appropriate way to respond on your part.
- ✗ Do not ignore the situation in the newsroom (this demoralizes the team).

Keep in mind: the first 24 hours are not about “handling everything”; they **are about support, safety, and minimizing harm.**

The study “Her Voice, Their Target,” conducted by Women in Media NGO in partnership with UNESCO in 2025, included a survey of 180 women media workers and found that **81% of Ukrainian women journalists have encountered online violence**, although women identify it as violence only in 64% of cases. In 14% of cases, the threats transitioned into the real world. The main consequences included deterioration of mental health, reduced ability to work, self-censorship.



Scan to learn more about the [Her Voice, Their Target study](#). 

The generalized guide “Steps for Newsroom to Take in the First 24 Hours Following an Online Attack against a Woman Journalist” is based on the practices of the following organizations: UNESCO (The Chilling), Coalition Against Online Violence, PEN America, Dart Center for Journalism and Trauma, IWWMF).

women in media.



Kingdom of the Netherlands

The guide has been prepared as part of the initiative “Strengthening the Resilience of Women Journalists in Ukraine: Countering Online Violence and Gendered Disinformation,” implemented by the Women in Media NGO with the support of the Ministry of Foreign Affairs of the Netherlands.