Internews

Digital security for journalists from marginalized communities

Women

Developed by Internews in collaboration with Lejla Sarcevic & Madeline de Figueiredo

Who is this guide for?

This guide highlights digital security considerations, mitigation strategies, and resources for women journalists who are concerned about their digital security, taking into account the different concerns of both the cis and trans communities. Additionally, the guidance in this resource is often relevant for individuals who belong to a different gender or no gender but may be perceived by others as being women or feminine. This guide is designed to be used by digital security specialists working with journalists who belong to this community, though some of its advice might also apply to journalists whose colleagues, sources, or other collaborators belong to this community.

Digital Security Challenges

Threats are the direct attacks that can impact your life.

Adversaries are the individuals executing these threats.

Vulnerabilities are the weaknesses in societal systems, technical systems, and individual habits that make it easier for attackers to carry out the threats. Systemic inequities are often the root cause of these weaknesses.

Threats	Adversaries	Vulnerabilities
• Harassment • Trolling • Stalking • Doxxing • Malware • Phishing	• Extremist groups • Individual trolls • Law enforcement or other authoritative entities • Misogynist groups • Former or current partners	• At a much higher risk of online harassment and trolling than men are, especially journalists who have very public facing roles or who work on beats traditionally seen as masculine. Trolls often try to get women to leave journalism altogether by making it very hard to stay therein.

	• Nation states	• Security professionals in newsrooms and beyond often pay less attention to women's concerns. • At a much higher risk of stalking and assault • Barriers to access to safe technologies and understanding of digital safety (gender digital divide) • Increasing criminalization of bodily autonomy and surveillance (e.g., crackdowns on reproductive rights and trans rights) • Lack of platform and law enforcement accountability discouraging reporting of incidents

Threat Modeling for Women Journalists

	Considerations for Women
Assets	Devices, communication with sources, physical safety, the ability to conduct journalistic work without the constant threat of trolling and harassment
Adversaries	Mostly non-state, though state or state-affiliated groups also often weaponize misogyny and transphobia
Likelihood	Women are more likely to be targeted than men, women are vulnerable to coercion and exploitation, and things like personal photos are more likely to be used against them. This risk is bigger for women who take on public facing positions, such as journalists.
Consequences	Consequences are often dependent on context but can include the following: harm to mental and physical health, risks to employment, self-censorship, punishment from community or family, and social ostracizing. There are potentially life-threatening consequences due to a strong overlap between digital security and personal security. Women may also feel the need to delete their social profiles or other personal information, which can be detrimental to the careers of individuals working in journalism.
Effort	Many women have personal information (including sensitive chats) on their devices. Managing this can require a lot of effort. Dealing with online harassment can also be incredibly time-consuming and draining.

Managing Digital Security for Women Journalists

Mitigation strategies are the practices that can be leveraged to address vulnerabilities.

- For example: quickly muting or blocking harassers on social media and elsewhere, using secure communications tools and disappearing messages, using a period tracking app that promotes and protects privacy, delaying posting photos so current location is not accessible, excluding maps/doors from photos of houses to mitigate risk of geolocation, making sure that home address is not publicly listed, blurring faces of dependents on social media posts, setting personal social media accounts to private and creating separate professional accounts for journalism work.

Mitigation tools are the devices, applications, and workflow apparatuses that can be applied to reduce the risk of attacks.

- For example: block/mute lists on social media to quickly identify harassers, password managers, social media privacy settings. Some physical safety apps can help send your geolocation to a trusted friend. Two factor authentication on important accounts, including email and social media, makes it very difficult for harassers to break into them.

Mitigation actors are the entities and individuals that can offer protection in a digital security context.

- For example: self, trusted friends, family, trusted healthcare professionals or other service providers, colleagues. There are also organizations specifically providing mitigation and emergency response support for women journalists such as the International Women's Media Foundation (IWMF).

How to Talk to and Persuade Others

Allies: Identifying allies to build communities and systems of good digital security practices. Allies in newsrooms are particularly crucial, since not all editors and security teams take issues such as online misogyny, harassment, or threats of doxxing seriously. It might be a good idea to work not just with women journalists but also with others (such as LGBTQ+ journalists or journalists from ethnic minorities) who might face similar threats.
Incentives: Incentivizing stakeholders to take up certain practices that promote better digital security habits. This could be as simple as pushing newsrooms and colleagues to take issues like harassment more seriously.
Transparency: Be transparent about challenges. Normalize that breaches do happen so that others feel comfortable speaking openly and sharing information about vulnerabilities, threats, attacks, etc.
Educate: Explain all pros and cons of certain digital security practices and be more direct about why adjustments would be beneficial. When talking to other journalists and other newsroom employees, lay out

what specific threats you are facing and what specific steps you could and they could take to mitigate those threats.
Communicate: Listen and learn from the community. Try to understand any hesitancy, address concerns, and be open-minded. Contextualize any tools or practices for the needs and profile of the community to make adoption and integration of digital security topics more accessible.
Nudge the Needle: Advocate for incremental changes and be willing to compromise for movement in a direction that promotes healthy digital security (e.g., moving primary form of communication from Facebook to a more secure platform, even if it is not the most secure platform). Remember that change takes time and institutions such as newsrooms can be a bit conservative.
Share Resources: Share tools, guidelines, and research from established and credible sources.

Digital Security Resources for Women Journalists

IWMF | Online Violence Courses and Resources

Hackblossom.org | DIY Feminist Cybersecurity

WizCase | Women's Guide to Cyber Safety 2023

Masaar | Digital Security for Women: Initiatives and Training Guides

PEN America | Online Harassment Field Manual