COFEM



Tip Sheet 1:

Digital Safety

Key Points



Digital violence is not a private problem. It is often used to silence, intimidate, and exclude women from public life.



Effective digital safety starts with understanding your risks. Ask what you are protecting, from whom, and what the consequences would be if information were exposed.



Strong passwords, two-factor authentication, secure communications, and privacy settings remain some of the most effective protections against digital harm.



Digital security is a collective responsibility. Shared organisational practices, clear response procedures, and support networks help protect entire teams and movements.



Digital safety and wellbeing go hand in hand. Responding to online harm requires technical, legal, psychosocial, and emotional support.



The goal is not to withdraw from digital spaces, but to participate in them safely, confidently, and on our own terms.

The Politics Of Being Online

The extraordinary thing about being online is how quickly people, ideas and information can move. Digital spaces allow us to move. We move between communities, languages, countries and conversations. We move ideas, evidence and stories. We find one another, build relationships, challenge dominant narratives, and mobilise collectively across borders.

But movement is never only about what we gain. The same digital spaces that enable connection, visibility, and collective action can also expose us to new forms of surveillance, harassment, and harm. Feminists across the world have long argued that violence against women is not a private matter but a systemic violation of human rights, a position reflected in international normative frameworks including the Declaration on the Elimination of Violence against Women, the Maputo Protocol, and CEDAW General Recommendation No. 35. The #MeToo movement was built on this legacy. Initiated in 2006 by activist Tarana Burke as a survivor-led initiative, it gained global visibility when the hashtag went viral on social media in 2017. Within weeks, millions of people across an estimated 85 countries had shared their stories online, demonstrating how digital spaces can connect individual experiences to collective action and social change.[1]

In Argentina, the #NiUnaMenos movement emerged in 2015 following the murder of 14-year-old Chiara Páez, a case that sparked widespread public outrage about femicide. A tweet by journalist Marcela Ojeda calling on women to raise their voices against gender-based killings quickly gained traction across activists, cultural, and media networks. Under the banner of #NiUnaMenos ("Not One Less"), the message spread rapidly through Twitter and Facebook, helping to mobilise hundreds of thousands of people in what became one of the largest feminist demonstrations in Latin American history. Like #MeToo, the movement demonstrated how digital spaces can transform individual experiences of violence into collective action and political pressure for change.[2]

These examples reveal something important: digital spaces are never neutral. The same technologies that enable feminist organising and collective action are shaped by power, politics, and competing interests. As the world becomes more connected, moving through digital spaces also exposes us to new forms of harm. The same technologies that allow feminist ideas to circulate can enable harassment, surveillance, misinformation, and abuse.[3] The same visibility that helps us build movements can make us targets. The same networks that nurture connections can also become channels through which violence travels.

For feminists working to end violence against women and girls (VAWG), the circulation of information, stories, and resources is one of our greatest strengths. We can document injustice, support survivors, learn from one another, and organise collectively across borders. But this digital transmission of knowledge also requires us to think carefully about safety, privacy, and risk. How, then, do we use digital power intentionally? How do we harness the possibilities that digital spaces create while minimising the risks they carry? How do we remain visible without becoming vulnerable? How do we protect ourselves, our organisations, and the people with whom we work, while continuing to participate fully in public life?

This Tip Sheet explores some practical answers to these questions. It moves from understanding digital violence as a political issue, to assessing risk, implementing practical protections, strengthening collective security, and responding to harm when it occurs.

[1] Sweeney J 2020

[2] https://8am.media/eng/ni-una-menos/

[3] Amnesty International, May 2021 *Azerbaijan: Stop the Vicious Campaign of Gendered Smears and Reprisals against Women Activists*. London: Amnesty International. Available at: https://www.amnesty.org

Spotlight

The case of Narmin Shahmarzadeh[4]

On 8 March 2021, Azerbaijani women's rights activist Narmin Shahmarzadeh was involved in organising an International Women's Day march in Baku. The following morning, she woke up to discover that her Facebook account had been hacked.

The attackers used her account to publish fabricated conversations and pornographic content. They gained access to her identification documents, used her government-issued ID to lock her out of her account, and stole her bank card to pay for advertisements promoting the abusive content. On Telegram, the perpetrators created a channel falsely attributing pornographic images to Narmin. Within a short period, the channel had attracted more than 1,600 subscribers and thousands of views.

The attack was digital, but its purpose was political. Narmin was targeted because she was visible. She had organised, spoken out, and challenged power. The attackers transformed the very tools that had enabled her activism into weapons against her. Her experience illustrates an increasingly common reality for women human rights defenders and feminist activists. Digital violence is often designed not only to intimidate individuals, but also to damage reputations, undermine credibility, disrupt organising efforts, and create conditions of fear. The consequences may begin online, but they rarely remain there.

The Cost Of Visibility

Narmin's experience is not an isolated case. It illustrates a broader pattern in which digital violence is used to punish visibility, disrupt activism, and restrict women's participation in public life. Increasingly, online abuse is not confined to digital spaces; it spills into the physical world, affecting women's safety, wellbeing, livelihoods, and ability to engage in public and political life.

The impact of digital harm on women in public life is both sweeping and escalating. A 2025 UN Women study involving over 640 women across 119 countries found that 70% of women human rights defenders (WHRDs), activists, journalists, and public communicators had experienced online violence in the course of their work, and the consequences do not stay online. Forty-one percent reported experiencing offline harm, including physical assault, stalking, and verbal harassment that they directly linked to violence that began in digital spaces. Among women human rights defenders and activists, that figure rose to 44 %. The trajectory from online to offline violence is also accelerating; for women journalists and media workers, the proportion connecting online violence to offline harm more than doubled between 2020 and 2025, from 20% to 42%. Nearly a quarter of all respondents had experienced AI-assisted online violence, with 28% of WHRDs and activists reporting the use of artificial intelligence technologies in the abuse directed at them. The report is unambiguous about what this violence is designed to do: it is a strategic instrument, deployed to suppress women's freedom of expression, obstruct their democratic participation, and roll back their rights to gender equality with effects that are, as the authors put it, anything but virtual.[5]

But recognising these risks should not lead us to retreat from digital spaces or accept violence as the price of participation. Women, girls, and gender-diverse people have the right to be visible, to express themselves freely, to build community, to organise, to create, and to experience joy online without fear of abuse. The goal is not to make ourselves smaller or less present in digital spaces, but to transform those spaces so that everyone can participate safely, equally and with dignity. Protecting ourselves online is therefore not only about reducing harm; it is also about defending the internet as a space for expression, solidarity, creativity, and feminist possibilities.

[4] Ibid
[5] Posetti et al., UN Women, December 2025

Assessing Your Risk

While governments, technology companies and digital platforms have the primary responsibility for creating safer digital environments, current protections and accountability mechanisms remain uneven. In this context, feminist organisations and activists may choose to take practical steps to help minimise risk. These measures cannot eliminate harm, nor should they shift responsibility away from those who perpetrate violence, but they can strengthen our ability to navigate digital spaces on our own terms.

Not every threat applies to every activist, organisation or movement. A feminist researcher handling survivor testimony faces different risks from a social media campaigner. A woman human rights defender documenting state violence faces different challenges from a service provider running a local support group. Rather than asking, "*What is the safest thing to do?*", a more useful question is: "*What am I trying to protect, and from whom?*"

For some organisations, the answer may be survivor information, case files or contact databases. For others, the priority may be protecting staff identities, securing communications, or safeguarding social media accounts. Individual activists may be concerned about doxxing, stalking, online harassment, or the exposure of personal information that could place them or their families at risk. There is no single approach that is right for everyone. Risk assessments are most effective when they reflect each person's context, priorities and level of public visibility, enabling informed choices about which protective measures are appropriate. Narmin Shahmarzadeh's experience illustrates how quickly a digital attack can escalate when personal information, identity documents and social media accounts are compromised. Understanding which information, relationships and accounts are most important to protect is therefore a useful starting point for reducing vulnerability and minimising risk.

A simple risk assessment can begin with four questions:[6]

- What information or assets am I trying to protect?
- Who might want access to them?
- What methods might they use?
- What would the consequences be if that information were exposed?

Most organisations do not have unlimited time, money, or technical expertise to prepare for every possible threat. Rather, the goal is to make informed decisions about the risks that matter most in your context and to prioritise your efforts accordingly. Once you understand your risks, it becomes much easier to identify the practical steps that will make the great difference.

[6] These questions draw on established threat-modelling approaches in cybersecurity, adapted to feminist digital safety practice. See, for example, Slupska et al's Participatory Threat Modelling, 2021



Securing Your Accounts And Devices

The most common entry point for serious digital harm is account takeover: someone gaining access to your email, social media, or other accounts through a stolen, guessed, or reused password. Once an email account is compromised, every other account linked to it becomes vulnerable. For feminist activists, researchers, and human rights defenders, the consequences can extend far beyond personal inconvenience, exposing sources, survivors, colleagues, and sensitive communications. Narmin Shahmarzadeh's experience illustrates how quickly an account compromise can escalate. Attackers gained access to her social media account, used her identity to distribute fabricated content, and locked her out of her own profile. What began as a digital intrusion quickly became a reputational and psychological attack.

The good news is that some of the most effective protections are also the simplest:

Use strong, unique passwords for every account and store them in a reputable password manager such as Bitwarden or 1Password. Password managers generate and remember complex passwords so that you do not have to, eliminating the common and risky practice of reusing the same password across multiple platforms.

Pair this with two-factor authentication (2FA) on every account that supports it. Where possible, use an authenticator app rather than SMS verification, which can be vulnerable to SIM-swapping attacks. Pay particular attention to your email account. It is the master key to your digital life and should be treated as your highest-priority account to protect.



Device security matters too. Keep your operating systems, browsers, and apps updated, as updates routinely patch vulnerabilities that attackers actively exploit. Enable full-disk encryption on laptops and use reputable antivirus software where appropriate. Be cautious with unexpected links, attachments, and login requests. Phishing remains one of the most effective ways of stealing credentials or installing malware.

The recommendations above provide a practical starting point, but digital security is not a one-time checklist. It is an ongoing practice that evolves alongside changing technologies and threats. A number of feminist organisations have developed accessible guidance tailored to the experiences of women, girls, and gender-diverse people. These include FRIDA's Digital Security Resources for Young Women, Gitbook, UN Women's Online Safety Guide, and the Youth Guide to End Online Gender-based Violence. These resources offer more detailed advice on strengthening digital wellbeing, responding to online abuse and building safer digital practices.

Managing Your Digital Footprint And Privacy

Every photograph, location tag, profile update, and social media post contributes to your digital footprint. For feminist activists and WHRDs, these seemingly small pieces of information can reveal far more than intended. Managing your digital footprint is not about becoming invisible. It is about being intentional. Start by reviewing the information you make publicly available. Lock down privacy settings on social media platforms, paying particular attention to who can tag you, search for you, or view your content. Review these settings regularly, as platforms frequently change their privacy defaults without notice.

Think carefully about location information. Real-time check-ins, geotagged photographs, and posts that reveal where you and your family live, work, or spend significant time can make it easier for others to track your movements. Smartphone photographs often contain location metadata by default, which should be removed before sharing sensitive images publicly.

For sensitive communications, use tools designed with privacy in mind:

- Signal remains one of the most trusted options for encrypted messaging and calls.
- For email, privacy-focused providers such as Proton Mail offer additional protections compared with conventional services.
- Review app permissions regularly and remove unnecessary access to your location, microphone, camera, and contacts.
- When working in public spaces, avoid accessing sensitive information over unsecured Wi-Fi networks, and consider using a trusted VPN if this is unavoidable.

None of these measures is particularly complicated. When applied consistently, however, they can significantly reduce exposure to risk.

Collective and Organisational Protection

Digital safety is often presented as an individual responsibility. However, within feminist organisations and movements, one compromised account can expose an entire team's communications, contacts, and work. One weak password on a shared platform can create vulnerabilities for all collaborators. Digital security, therefore, needs to be understood as a form of collective care rather than an individual matter of competence. This begins with establishing shared practices. Agree on which tools will be used for sensitive communications, set minimum expectations around passwords and two-factor authentication, and ensure that organisational accounts do not depend on a single person's device or profile.

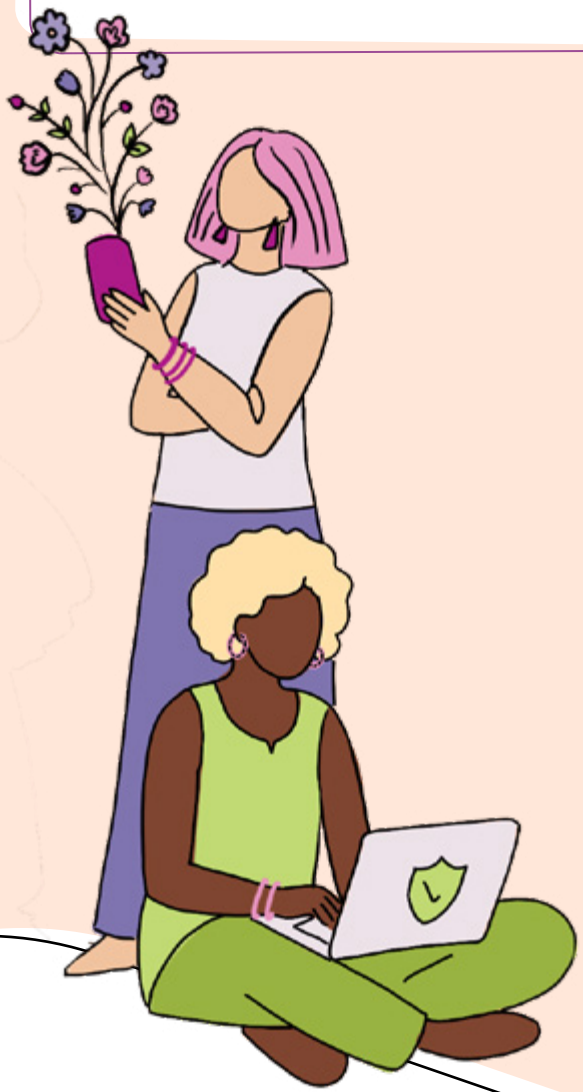
When staff leave an organisation, access to shared accounts should be removed promptly and routinely. Equally important, build support structures before they are needed. Identify trusted people within your networks who can provide technical assistance, legal advice, or psychosocial support if you or someone you know is targeted. Develop simple internal procedures for responding to incidents such as hacking, doxxing, or account compromise. Knowing who will do what during a crisis can dramatically reduce confusion and harm. Feminist organisations routinely invest in the physical safety and wellbeing of their staff and communities. Digital safety deserves the same attention.

Responding To Incidents and Prioritising Wellbeing

Digital attacks and online harassment are often most damaging when people have no plan for responding to them. Establishing a basic response framework before an incident occurs can make a difference.

Document

When harassment or an account compromise occurs, document first. Take screenshots, save URLs, record usernames, and preserve evidence before content is deleted or removed. This documentation may be critical for platform reports, legal action, or police complaints.



Report

Know where to seek support. Platform reporting mechanisms are imperfect, but they remain an important first step, particularly in cases involving threats of violence, impersonation, stalking, or image-based abuse. Many countries have organisations that provide legal, psychosocial, or technical support to activists experiencing digital harm. Familiarise yourself with these resources before a crisis occurs and keep contact details easily accessible.

Care

The emotional impact of digital harm is consequential. Sexualised abuse, fabricated content, coordinated harassment campaigns, and sustained threats are designed to exhaust, isolate, and intimidate. Their effects are real, cumulative, and often invisible to others. For this reason, digital safety planning should always include care. Talk to trusted colleagues. Take breaks from social media when needed. Use mute, block, and restrict functions without apology. Seek professional support if the impact becomes overwhelming. Digital security and wellbeing are not separate concerns. They are two parts of the same commitment: ensuring that feminist activists, organisations, and movements can continue their work safely, sustainably, and on their own terms.

Visibility, Safety And Power

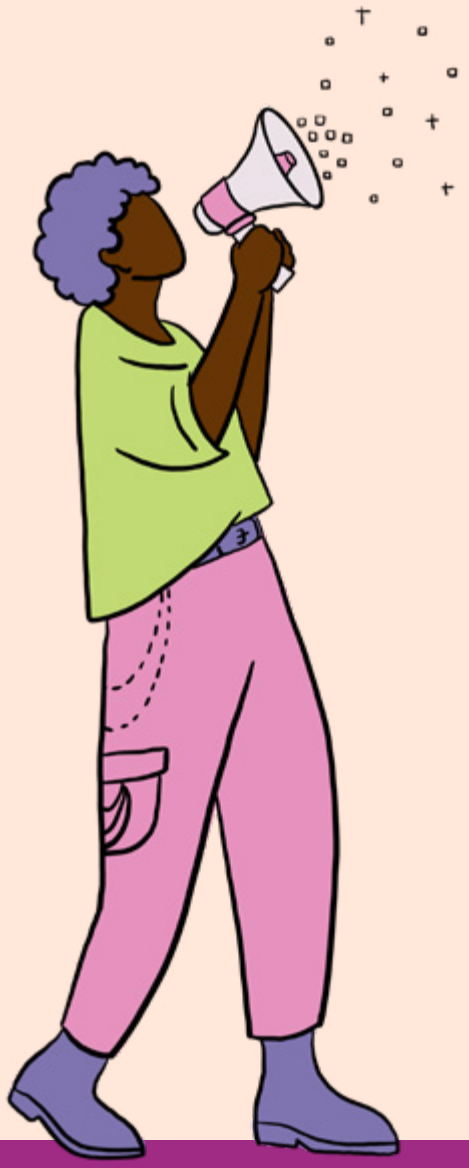
Digital safety is about participating in public life on our own terms. Feminist movements have always had to adapt to changing political landscapes by finding new ways to organise, communicate, and build power. Today, digital spaces are part of that landscape. They allow us to share knowledge, support survivors, challenge injustice, and connect across borders in ways that would have been unimaginable a generation ago. Yet they also create new risks that require attention, preparation, and care.

The goal is to make informed choices about risk, strengthen collective protection, and build the confidence to continue participating in digital spaces safely and strategically. Thus, digital safety is both a technical issue and a movement issue. When feminist activists, organisations, and communities can communicate securely, protect one another, and respond effectively to harm, they are better able to sustain the work of advancing rights, supporting survivors, and creating change. Our movements depend on connection. Digital safety helps ensure that those connections remain a source of strength rather than vulnerability.

Resources

The following organisations and resources offer free, practical digital safety support

Resource	What it offers
Access Now Digital Security Helpline	Free, confidential digital security support for activists, journalists, and human rights defenders globally — including South Africa.
Coalition Against Online Violence (CAOV)	Resources and support specifically for women journalists and gender-based online harassment.
PEN America Online Harassment Field Manual	Comprehensive practical guidance on responding to online harassment — free online.
Cyber Civil Rights Initiative	Support for survivors of non-consensual intimate image abuse; legal resources and platform reporting guides.
Electronic Frontier Foundation (EFF) — Surveillance Self-Defence	Free, practical security guides for activists and journalists by threat level.
Front Line Defenders	Digital security and protection support for human rights defenders globally.
Feminist Tech Exchange	Technology and digital security resources created specifically for feminist organisations.



Acknowledgements

This piece was written by Joy Watson and reviewed by Jennifer Chinoye Amadi, Leah Goldmann, Lauren Messina, and members of UN Women's EVAW team, designed by Amarawati Ayuningtyas and Léa Drougard, and illustrated by Sarah Imran. This publication was produced by COFEM under the EU-funded UN Women ACT to End Violence Against Women and Girls Programme. Its contents are the sole responsibility of COFEM and do not necessarily reflect the views of the European Union or UN Women.

Suggested Citation

Coalition of Feminists for Social Change. Tip Sheet 1: Digital Safety, *Bytes of Resistance: Addressing Technology-Facilitated Gender-Based Violence* (2026).

References

Amnesty International (2021) *Azerbaijan: Stop the vicious campaign of gendered smears and reprisals against women activists*. London: Amnesty International. Available at: https://www.amnesty.org

Andreasen, M.B. (2020) 'Feminist/activist responses to online abuse', in The International Encyclopaedia of Gender, Media, and Communication. Hoboken: Wiley.

Andreasen, M.B. (2024) 'Evidentiary activism in the digital age: on the rise of feminist struggles against gender-based online violence', in Edited volume title. London: Routledge.

Bansal, V., Eruyar, S., Wang, S. & Wessells, M. (2024) 'A scoping review of technology-facilitated gender-based violence in low- and middle-income countries across Asia', Trauma, Violence, & Abuse, online.

Bennett, L. and Livingston, S. (2020) 'The #MeToo movement, digital media and the public sphere', in Digital Media and the Public Sphere. London: Routledge.

Koch, L., Russo Riva, M.P. & Steinert, J.I. (2025) 'Technology-facilitated gender-based violence against politically active women: A systematic review of psychological and political consequences and women's coping behaviours', Trauma, Violence, & Abuse, online.

Loney-Howes, R. and Mendes, K. (2023) 'It's a global #MeToo: A cross-national comparison of social media responses to sexual violence', Feminist Media Studies, 24(7), pp. 1032–1050.

Posetti J, Hellmueller L, Williams K, Renaud P, Aboulez N and Shabbir N 2025 *Tipping Point: The Chilling Escalation of Online Violence Against Women in the Public Sphere*, UN Women, New York.

UN Women (2025) AI and anonymity: Digital violence against women in the age of online backlash. New York: UN Women.

VAWG Helpdesk (2017) Cyber VAWG: Violence against women and girls and information and communications technology. VAWG Helpdesk Research Report No. 211. London: UK Aid.

Slupska J, Dawson S, Ma L and Neff G (2021) Participatory Threat Modelling: Exploring Paths to Reconfigure Cybersecurity. Proceedings of the ACM on Human-Computer Interaction.

Sweeney J 2020 The *#Me Too Movement in Comparative Perspective, Journal of Gender, Social Policy and the Law*, Volume 29, Issue 1, 2020

Organized Crime and Corruption Reporting Project (OCCRP) (2023) 'How revenge porn is used to silence dissidents in Azerbaijan', OCCRP, 3 April. Available at: https://www.occrp.org/en/feature/how-revenge-porn-is-used-to-silence-dissidents-in-azerbaijan