FEMME FORTE

Digital Safety and Wellbeing Toolkit

Femme Forte Uganda is powered by community, care, and collective action.

To connect, collaborate, or learn more about our work, reach out:

TELEPHONE: +256 393 224 051

EMAIL: info@femmeforteug.org

WEBSITE: www.femmeforteug.org

About Femme Forte

Femme Forte is a feminist movement-building entity and social enterprise committed to advancing the economic, social, and political power of women in Uganda. We blend advocacy with innovation, developing sustainable models that resource our work and create opportunities for young women to thrive.

We exist to strengthen pathways between young and older women who aspire to meaningfully contribute to the broader women's movement in Uganda. Femme Forte believes in the power of community. We love and uphold one another, guided by a shared commitment to sisterhood and collective growth. We hold each other accountable, act in one another's best interests, and create spaces where women can lead, heal, and thrive.

Our Vision

A balanced society that provides equal opportunity to men and women.

Our Mission

Foster effective resilience to break barriers and reach new heights for women in Uganda

Our Values

Our values are summarized in the word SAFE, which reflects the principles that guide our work and relationships.

S — Sisterhood and Partnership

We care and are loyal to one another

We believe in community- can't do it alone

We love and uphold one another

We have each other's best interests at heart

A — Accountability

We have nothing to hide, what you see is what you get

We share our stories regularly; there is no room for surprises

We are open to counsel, rebuke and intentional growth

F — Feminist Leadership

We create safe environments for expression, self-care, participation and growth of leadership skills

We are aware of ourselves as part of a larger whole

We are relational and inspirational with an orientation towards transformation

We are aware and attentive to power dynamics and their varied meanings in context to culture and identities

E — Equity

We believe we are human first, then women thus equity is important to us

16 Days of Activism & Digital Safety

The 16 Days of Activism Against Gender-Based Violence (Nov 25–Dec 10) is an annual global campaign calling for the prevention and elimination of violence against women and girls.

In 2025, the UN-led campaign theme is “UNiTE to End Digital Violence Against All Women and Girls”, recognizing that online spaces have become a battleground for gendered abuse; from harassment and doxxing to image-based violence and coercive control.

Online abuse silences women and girls. There is no excuse, and no justification.
Image by UN Women

For Femme Forte, digital safety is part of our mission to foster resilience and break barriers. It is gender justice in action.

As we observe the 16 Days, we can:

- Raise awareness in our networks;
- Build digital solidarity by organizing collective trainings, peer support spaces, and shared learning sessions;
- Advocate for change, both within our communities and in broader policy or platform arenas;
- Center care, offering check-ins, emotional support, and digital wellbeing practices to sustain resilience beyond the campaign.

Toolkit Overview

Purpose of the Toolkit

The Femme Forte Digital Safety and Wellbeing Toolkit is a practical guide designed to equip activists, advocates, and organizations with the knowledge and tools to strengthen their digital safety, security, and wellbeing. It provides accessible, step-by-step strategies for protecting personal and organizational data, responding to online threats, and promoting care-centered online practices.

Intended Users

- Women's rights advocates and community organizers
- Civil society organizations and digital activists
- Journalists, artists, and human-rights defenders
- Students, researchers, and community trainers

How to Use the Toolkit

The toolkit can be used as both a self-study resource and a training guide.

Each section can stand alone, covering topics such as online harassment, data protection, or organizational safety, or be used as part of a broader learning journey toward holistic digital wellbeing.

Toolkit Structure

The Femme Forte Digital Safety Toolkit is organized into 9 easy-to-follow sections. Each part builds progressively from awareness to action.

Introduction

- Understanding Digital Threats
- Digital Security Basics
- Privacy and Data Protection
- Online Harassment and Self-Protection
- Safe Organizing Online
- Tools and Resources
- Feminist Digital Wellbeing
- Emergency Response Plan
- Appendices

Acknowledgements

The Femme Forte Digital Safety and Wellbeing Toolkit was conceptualized, written, and designed entirely by the Femme Forte team. It reflects our shared commitment to advancing women's safety, leadership, and wellbeing in an increasingly digital world.

We acknowledge the creativity, dedication, and expertise of every team member who contributed research, content development, design, and review support to bring this resource to life. This toolkit is a product of collective effort, care, and persistence built from our own experiences navigating digital spaces and supporting others to do so safely.

We extend deep appreciation to the women within the Femme Forte network whose passion and resilience continue to inspire our work. This toolkit is dedicated to all women striving to make digital spaces safer, more inclusive, and more empowering for themselves and their communities.

Together, we reaffirm our belief that safety is not just individual; it is collective, and it is essential to the strength of our movement.

Disclaimer and Usage Note

This toolkit is intended for educational and advocacy purposes. The information provided is based on best practices in digital safety and wellbeing but does not constitute legal, technical, or professional advice. Users are encouraged to adapt the recommendations to their specific contexts and exercise discretion when applying digital safety measures. Femme Forte is not liable for any misuse or misinterpretation of the information contained herein.

Why Digital Safety Matters

Digital spaces hold immense potential for feminist connection, storytelling, and advocacy. They allow us to organize, create, and amplify our movements across borders. Yet these same spaces are also marked by surveillance, harassment, and violence. Queer women, activists, and feminist organizations are targeted precisely because their visibility challenges systems of power.

Building digital resilience is not just about technology; it's about care, solidarity, and survival. A feminist approach to digital safety centers community over fear, and collective protection over isolation.

Guiding Principles

- Feminist Care: Safety is an act of love and collective responsibility
- Autonomy: We have the right to control our data, identities, and digital presence.
- Solidarity: Protecting ourselves protects our communities.
- Empowerment: Technology should serve liberation, not fear.

Understanding Digital Threats

Safety online is a right, not a priviledge.
Image by UN Women

Awareness is the first step to resistance. Digital threats are not random; they are deliberate tools of power used to silence, intimidate, and erase women, queer persons, and feminist movements. Online violence reproduces the same patriarchal control that exists offline, only now through technology.

For feminist activists, journalists, and community organizers, understanding these threats is an act of survival and collective care.

Common Threats

Online Harassment & Doxxing

Women in public life, from activists to journalists often face coordinated trolling, sexualized insults, and threats of rape or death. Indian journalist Rana Ayyub was doxxed and subjected to deepfake pornography after criticizing state violence (United Nations Human Rights Office of the High Commissioner, 2018). Her experience shows how online attacks are used to punish women's speech and silence dissent.

Hacking & Phishing

Activists and human rights defenders are frequently targeted through fake login pages or malicious links. In 2021, the Pegasus spyware scandal revealed that activists and journalists in multiple countries had been targeted with phone malware (BBC News, 2021). Pegasus infects iPhones and Android devices, allowing operators to extract messages, photos and emails, record calls and secretly activate microphones and cameras.

Surveillance & Tracking

Governments and abusers use surveillance technology to monitor women's movements and communications. LGBTQ+ activists in Egypt, for example, have reported being tracked through dating apps and social media (Holleis, 2023). Surveillance is not just state control; it's a digital form of stalking that violates autonomy and safety.

Data Leaks & Breaches

A data leak can expose the identities of survivors, informants, and feminist collectives. Such breaches compromise privacy, disrupt operations, and put individuals and organizations at risk. Protecting sensitive information is essential, and privacy is a form of protection.

Disinformation & Defamation Campaigns

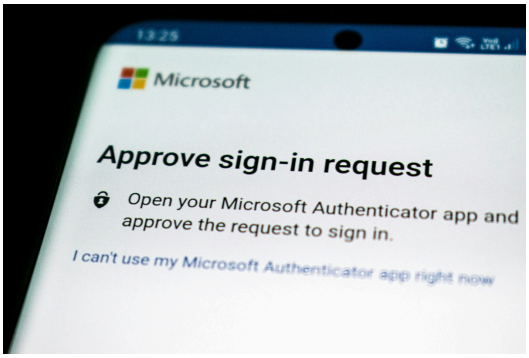
Feminist leaders are often targeted with coordinated misinformation designed to erode credibility. In 2021, several Nigerian women activists who organized #EndSARS protests were falsely accused online of money laundering and "foreign influence" (Dim, 2023). Such disinformation discredits feminist causes and deters participation.

Digital Security Basics

Digital security isn't just about technology; it's about protecting our voices, tories, and movements. Every password, setting, and decision we make online shapes how power moves through our spaces. These steps are not just precautions; they are acts of care and resistance.

Strong Passwords & Authentication

- Use long, unique passwords (12+ characters) for each account.
- Consider a password manager like Bitwarden or 1Password to safely store them.
- Turn on Two-Factor Authentication (2FA) wherever possible, even if it feels tedious. It's an extra lock between you and a hacker.
- Avoid sharing passwords, even within trusted circles. Shared safety doesn't mean shared access.



Secure your devices and accounts to safe- guard your activism. Image by Ed Hardie on Unsplash

Device Protection

- Your phone and laptop are extensions of you. Keep them protected.
- Keep your software updated. Updates fix security holes that attackers exploit.
- Install antivirus and firewall protection to reduce risks of infection.
- Always lock your devices with a PIN, password, or fingerprint.

- Avoid using public Wi-Fi for sensitive activities. If you must, use a trusted VPN.
- Back up your files regularly

Remember: ***A secure device means uninterrupted activism.***

Secure Communication

- Our words are political. Protect them as you would your personal safety.
- Use encrypted messaging apps like Signal, Element, or Session.
- On WhatsApp, enable disappearing messages and limit who can add you to groups.
- Be cautious with unknown links or attachments. Phishing is one of the most common attacks
- Avoid sharing sensitive details (like addresses or contacts) through unverified or public channels.

Feminist practice: ***Encryption is not secrecy, it's care. It keeps our organizing safe from surveillance.***

Safer Social Media Use

- Social media is a double-edged sword: a megaphone for activism and a window for harm. Use it consciously.
- Review your privacy settings every few months. Platforms change policies silently.
- Limit personal details such as location, workplace, or family names in bios.
- Blur faces or identifying details when posting images from protests or meetings.
- Consider using pseudonyms or separate accounts for activism to manage risk.
- If you face harassment, document, block, and report, and lean on your networks for support

Solidarity note: ***Visibility is power, but safety is strategy. You get to decide how you show up online — no explanation needed.***

Reflection Prompt

- What forms of digital violence do you recognize in your context
- How can your community create rapid-response systems to support those under attack?
- What lessons can we learn from feminist movements that turned digital threats into collective strength?

Privacy and Data Protection

Privacy is not secrecy; it's self-determination. For feminists, protecting data is about protecting stories, movements, and communities. Our archives, messages, and photos are part of our collective history. Keeping them safe is an act of love and resistance.

Digital privacy is also political: states, corporations, and abusers often exploit data to surveil, control, or discredit feminist voices. Reclaiming our digital autonomy means deciding what to share, what to protect, and who gets access.

Managing Data

Before you can protect information, you must know what you hold.

- Audit your data regularly: What personal or organizational information do you store? Who has access to it?
- Collect only what's essential. Less data means fewer risks.
- Delete outdated files and duplicates to reduce digital clutter.
- When in doubt, ask for consent before storing or sharing others' information.

Secure Storage

- Where you store your data matters. Make it harder for intruders, even digital ones, to find or misuse your work.
- Use encrypted drives or folders like VeraCrypt or Cryptomator for sensitive files.
- For cloud storage, choose secure, privacy-respecting platforms such as Proton Drive or Tresorit.
- Avoid storing activist or survivor data on shared public drives (like Google Docs or Dropbox).
- Maintain offline backups on external hard drives or USBs kept in safe physical locations.

Encryption

Encryption keeps your communications and files safe from prying eyes. Think of it as wrapping your message in care before sending it out into the world.

- Encrypt sensitive files before sharing them through email or cloud platforms.
- Use secure file transfer tools like OnionShare or Send Anywhere (instead of email attachments).
- When sending passwords or sensitive links, share them through separate channels for example, send the password via Signal, not in
- the same email as the file.

Reflection Prompt

- What information do you currently hold that could put you or your community at risk if exposed?
- How can you create feminist data care practices like collective audits or safety check-ins, within your organization or network?

Online Harassment and Self- Protection

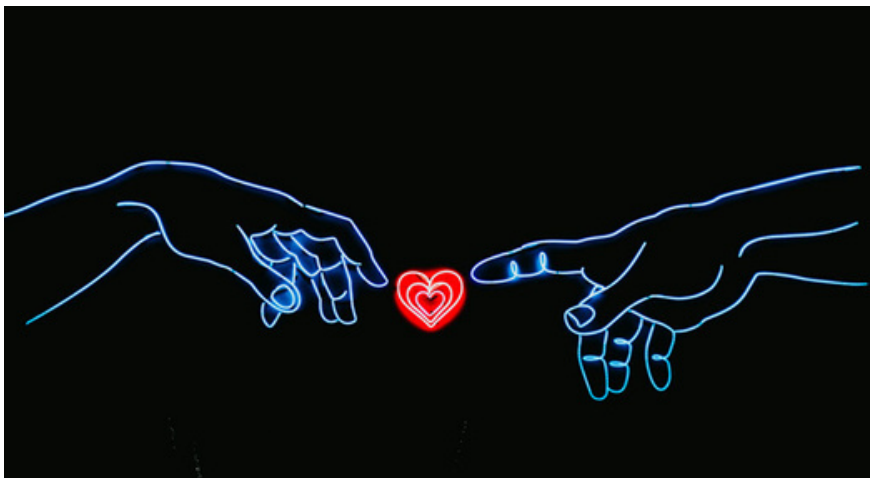
Understanding Online Violence

Online abuse isn't always obvious. Sometimes it comes as direct attacks like threats or hateful messages. Other times, it's more subtle—someone might spy on you, impersonate you, or spread false information about you. Even when it's not physical, this kind of abuse can wear you down emotionally, causing stress, anxiety, and fatigue. Recognizing these effects as real harm is the first step in taking care of yourself.

How to Respond

- Keep a record: Save screenshots, messages, and links. These can be useful if you need to report the abuse.
- Block and report: Don't hesitate to use the tools platforms provide to stop harassers from reaching you.
- Tell someone you trust: Sharing what's happening with a friend, family member, or colleague gives you support and ensures you're not facing it alone.
- Don't engage trolls: People who harass online often want attention or a reaction. Responding can make things worse.
- Take care of your mental health: Talking to a counselor, joining a support group, or practicing self-care is not a luxury; it's a part of resisting abuse.

Looking After Each Other



You are not alone! Safety is solidarity, not isolation.
Image by Devin Avery on Unsplash

We're stronger together. Some ways to protect ourselves collectively include:

- Creating clear response plans within organizations or communities so everyone knows what to do if harassment happens.
- Sharing safety tips regularly to help each other stay aware and prepared
- Taking breaks from screens and social media when needed; stepping back can help recharge your energy and protect your wellbeing.

Remember: ***protecting yourself online isn't just about technology, it's about your emotional safety, your dignity, and your power to continue speaking, creating, and connecting without fear.***

Safe Organizing Online

Hosting Secure Meetings

Running meetings online can be convenient, but safety is key. Some ways to stay secure include:

- Choose trusted platforms: Use video tools like Jitsi, Zoom (with passwords), or BigBlueButton.
- Keep links private: Share meeting links only with invited participants to prevent uninvited guests.
- Record carefully: Only record when it's necessary, and always consent from everyone involved. get

Managing Online Communities

Whether you're leading a discussion group or organizing virtually, keeping spaces safe matters:

- Moderate actively: Ensure everyone engages respectfully and that harmful behavior is addressed quickly.
- Set community agreements: Make clear rules for online discussions so everyone knows what's acceptable.

Protecting Collective Archives

Your group's knowledge and records are valuable.Protect them like you would any important resource:

- Store sensitive files safely: Keep them offline or in encrypted storage.
- Control access: Give permissions carefully, so only trusted members can view or edit important archives.

Tools and Resources

Feminist and Digital Rights Resources

For activists, feminist organizers, and anyone navigating online spaces, having reliable sources of support and guidance is critical. These organizations provide expertise, training, and emergency assistance to help protect your safety, privacy, and digital presence:

Her Internet

HER Internet provides training in digital safety and cybersecurity, conducts research on how algorithms and surveillance impact marginalized communities, and creates safe spaces for collective care and peer support. HER Internet emphasizes not just personal protection, but community resilience and feminist advocacy online, in Uganda.

Unwanted Witness

Unwanted Witness promotes online freedoms and protects digital rights in Uganda. The organization advocates for privacy, digital identity, digital inclusion, and freedom of expression, while empowering citizens to use technology safely and holding institutions accountable for digital rights violations.

Digital Woman Uganda

DWU is a civic-tech, feminist, and digital rights advocacy organization that provides digital literacy skills to women and girls in both urban and rural areas in Uganda. Their work spans digital literacy training, advocacy for gender-sensitive digital policies, promoting access to digital tools, and conducting research to inform innovative solutions

Safe Sisters

A fellowship program for women human rights defenders, journalists or media workers, and activists that trains them to understand & respond to the digital security challenges they face in their work and daily life

Access Now

Access Now provides a digital security helpline for activists worldwide, helping those who face urgent threats online. They offer toolkits, guides, and step-by-step advice on encryption, secure communication, and protecting sensitive data. Their work is particularly useful for anyone facing coordinated online attacks or state-level surveillance.

APC (Association for Progressive Communications)

APC is an international network using information and communication technologies (ICTs) to promote peace, human rights, and development. Their work aims to decolonize the internet and challenge inequality, with a strong focus on empowering marginalized communities, promoting digital rights, and advancing feminist and social justice agendas online.

Digital Defenders Partnership (DDP)

DDP supports activists at risk by providing emergency assistance, digital security training, and strategic guidance. They specialize in helping groups manage threats in high-risk contexts, from targeted harassment to political surveillance.

Note: ***The organizations listed above are examples of resources available to support digital safety, security, and feminist advocacy. This is not an exhaustive list; there are many other local, regional, and global initiatives doing important work in digital rights, online protection, and feminist empowerment. Users are encouraged to explore additional resources that best fit their context and needs.***

How to Make the Most of These Resources:

- Stay updated: Follow their blogs, newsletters,or social media for the latest tips, tools, and alerts on digital safety.
- Engage with their training: Many of these organizations run webinars, workshops, or peer learning sessions, participating can improve your security practices and build networks of support.
- Reach out in emergencies: Don’t wait until a problem escalates. These organizations are there to provide practical, immediate support when you face online threats.
- Share knowledge: Use what you learn to educate your community, building collective resilience and safer spaces for everyone.

Feminist Digital Wellbeing

Digital safety isn't just about tools and technology. It's also about care, boundaries, and emotional wellbeing. Protecting yourself online means taking care of your mind, body, and community, not just your data.

Your well being comes first. It's okay to skip notifications and take space for yourself.

Boundaries Online

- Take breaks from social media: Stepping away from constant notifications helps prevent burnout and emotional fatigue.
- Set limits on notifications: Only allow alerts from people or platforms that truly matter to you.
- Use anonymous browsing: Tools like private or incognito modes can help reclaim privacy and reduce unwanted tracking.

Collective Care

- Normalize rest and emotional check-ins: Make it okay to pause, breathe, and share how you're feeling with your peers.
- Build solidarity groups: Create networks where feminist organizers or activists can support each other, share resources, and troubleshoot digital challenges together.

Healing in Digital Spaces

- Remember vulnerability is not weakness: Acknowledge your feelings without shame; they are part of your power.
- Share affirmations and safety reminders: Positive messages and gentle guidance can strengthen both individual and collective resilience.
- Center joy and creativity in feminist tech work: Don't let digital safety be all stress. Celebrate successes, create, and nurture spaces that are
- inspiring and affirming.

Emergency Response Plan

Emergencies can happen online, just like in the physical world. Being prepared with clear steps can help you respond calmly, protect yourself, and minimize harm.

If You Are Hacked

- Disconnect immediately: Unplug or turn off your device from the internet to stop further intrusion.
- Change passwords securely: From a trusted device, update all passwords, especially for sensitive accounts like email, cloud storage, or social media.
- Notify your network: Inform allies, IT support, or digital security contacts in your community so they can provide guidance and help prevent further damage.
- Scan and update: Run malware and antivirus scans, update your software, and check for any unusual activity or unknown accounts.
- Report and document: Keep records of what happened, including suspicious messages, logs, or notifications, and report the incident to
- relevant platforms or authorities if needed.

If Facing Online Harassment

- Do not respond: Engaging attackers often escalates the situation. Silence can protect your wellbeing.
- Save evidence: Take screenshots, note URLs, and keep timestamps of all abusive interactions.
- Report to platforms: Use the platform's reporting tools to flag harassment or abuse.
- Reach out for support: Contact trusted peers, solidarity networks, or legal aid groups for guidance, emotional support, and next steps.

Checklist: Personal Digital Safety

Use this checklist to ensure your personal devices,accounts, and online presence are secure:

1. Strong, unique passwords for all accounts, with two-factor authentication (2FA) enabled
2. Devices updated regularly and secured with passcodes, PINs, or biometric locks
3. Secure messaging apps used for sensitive communications
4. Sensitive files encrypted and stored safely
5. Regular backups maintained, offline or in secure cloud storage

Checklist: Organizational Safety

This checklist helps ensure your team or organization maintains good digital security practices:

1. Shared password policy in place for team accounts
2. Defined data access levels so only authorized members can access sensitive information
3. Documented incident response plan for hacking, harassment, or data breaches
4. Digital security refresher sessions held quarterly for all team members