

FIELD

Practical Steps
to Navigate
Online
Harassment,
Disinformation
and Hate for
Women in
Politics





For a
digital
version
of this
guide

IIII Online attacks against women and gender-diverse people in politics and women public figures are globally common across diverse social and political landscapes.

While addressing this challenge can feel like an immense task, it's important to remember you are not alone: from sports to entertainment to politics, women face online harassment, targeted hate and disinformation. You can mitigate the impact through practices to enhance digital safety, cultivate peer and expert support, and develop communication and crisis prevention strategies to evaluate risk and respond to attacks.

Many of these recommended practices build on resilience strategies women and underrepresented groups in politics already deploy regularly in their professional and personal lives. Due to the complexity and context-heavy nature of these attacks, no sector has developed a comprehensive solution to address these multifaceted challenges, however, the ecosystem of support and awareness for elected officials and journalists is robust and ever-advancing.

Table of Contents

ALWAYS-ON SAFETY SETUP	<u>07</u>
Steps to secure your accounts	
<hr/>	
DOS & DON'TS	<u>11</u>
Strategies to help you diffuse, deflect and disentangle	
<hr/>	
SCENARIO PLAYBOOK	<u>17</u>
Stepping Into Public Life	<u>19</u>
My Data or Account Has Been Compromised	<u>25</u>
Doxxed or Deepfake Leak	<u>29</u>
Harassment or Disinformation Wave	<u>33</u>
Legal or Emotional Support	<u>39</u>
<hr/>	
SOCIAL MEDIA COMPANY AND CELL PHONE GUIDES	<u>43</u>
<hr/>	
DEEP-DIVE LIBRARY	<u>53</u>
Research, case studies, geek-level references	
<hr/>	
UNDERSTANDING THE PROBLEM	<u>85</u>
The numbers and stories behind the guide	

Always-On Safety Setup

Tick every box—and make sure you understand why each step matters. These basics are non-negotiable. If one of the later scenarios hits and these items aren't in place, fixing the problem will be much harder and slower. Treat this list as part of your regular digital routine and don't skip a single step.

Passwords for phone and computer

Set up a strong password/passcode for devices to secure your data if it is lost or stolen.

Enable Software Updates

These protect your devices and accounts from hackers and malicious software.

Enable Back up, Find & Remote Wipe for Devices

Enable automatic backups from your mobile device to iCloud or Google Drive if your device is lost, damaged, or stolen. Install a find my iPhone/iPad/Mac (with 2FA for iCloud) or Google's Find My Device to locate or wipe data from your lost device.

Password managers

Use a reliable one for team and personal accounts to securely generate, store and access strong passwords from anywhere.

Enable two-factor authentication (2FA)

Individual platforms allow users to set up 2FA, which grants access to an account or application only after successfully presenting two or more pieces of evidence of ownership. Text messages, emails and/or authentication apps provide codes.

Separate personal and public accounts

For social media, have different accounts for personal and work. Ensure privacy settings match the needs of your account (i.e. personal accounts set to private). Consider having different phones and computers for personal and work if possible.

Use a Virtual Private Network

Encrypt your access to the internet and communications via Virtual Private Networks (VPNs), and password protected WiFi. Never use public WiFi or WiFi with widely shared passwords, as it can be easily monitored. Consider trustworthy VPNs like ProtonVPN, TunnelBear, Mulvad or DuckDuckGo.

Anti-Doxxing/Privacy Monitoring Services

Consider hiring professional services to remove personally identifiable information or other personal data such as address or family information from the internet for proactive doxxing and data leak prevention.

Do's and Don'ts

Being the focus of disinformation hate can be overwhelming, however, these strategies can help you diffuse, deflect and disentangle yourself from disinformation and hate.

Countering Disinformation and Hate

DON'T

Don't keep it to yourself. Share what's going on with your team, inner circle or trusted network so they can support you. You are not alone and you don't need to have all the answers before reaching out to them.

Don't amplify or link to false claims. Instead, amplify the content you want to spread, keep it simple and make it visual. Redirect your audience to factual, independently verified resources when appropriate.

Don't say "no comment," instead, keep responses "short and sharp." "No Comment" leaves the impression you have something to hide, but a "short and sharp" response is effective to redirect and dismiss disinfo. Center your constituents and their values in your response whenever possible.

Don't engage with legitimate threats to your own safety, instead, monitor, document and report it. Don't engage with content that threatens your security, as your safety and containment/deescalation is key.

DO

Do check your resilience. Before you take action, pause to survey your physical and emotional capacity at this specific moment. Take simple actions to ask for help to monitor the situation, and pause to eat a meal, exercise, or go outside.

Do evaluate risk and virality to help determine physical threat level and identify what you need to protect (threat modeling). Consider appropriate levers to pull (i.e. report to authorities, report on social media platform channels, monitor but not respond, counterspeech, crisis communications or features to mute, block or restrict content).

Do consider counterspeech to de-escalate and de-personalize: Remember that these attacks aren't necessarily about you, they are about disenfranchising underrepresented groups from democratic processes. Counterspeech is a response that seeks to undermine harmful content, like organized campaigns, direct or indirect one-off responses. Review these counterspeech guidelines, and remember that counterspeech can come from allies, supporters, non-political institutions or bipartisan allies. Your networks can validate credibility, counter false claims, or do other online bystander Interventions.

Do speak plainly and directly, avoiding heavy legal or technical jargon can be off-putting. Use anecdotes and examples to demystify relevant issues.

DO

Do provide a “logic correction” instead of a “factual correction” that puts the focus on motives, networks & tactics. Fact checks are not effective at scale against disinfo.

Do map your Trusted professional networks, media and peer support networks. Peers can provide holistic, strategic and timely feedback. Professional networks can also validate credibility, contribute to strategy, and counter false claims. Do consider non-political entities and unlikely allies to cultivate relationships with, such as respected civil society groups and members of the media. Support from unlikely allies can confound attempts by disinformation actors to sow discord between groups they want to place in opposition.

Do implement team social media monitoring: Designate team members to review mentions and trends to escalate only the most important or risky issues to you. It can be as simple as searching terms or really complete.

Do Crisis Communications Preparation. Have a plan to address likely themes or pain points from adversaries, and know who you'll call for validation or in an emergency if needed.

Scenario Playbook

Turn here the moment something concrete happens. Each scenario hands you the right tools, hotlines, and step-by-step moves for that exact situation.

Find the scenario that matches what's happening and jump straight to its resources.

Stepping Into Public Life	<u>19</u>
My Data or Account Has Been Compromised	<u>25</u>
Doxxed or Deepfake Leak	<u>29</u>
Harassment or Disinformation Wave	<u>33</u>
Legal or Emotional Support	<u>39</u>

Stepping Into Public Life

Prepare your team and protect accounts

DIGITAL SECURITY GUIDES

Foundations for protecting your information

OnlineSOS Digital Security Risk Assessment Checklists:

Easy checklists help you understand and identify what you need to protect (threat modeling) and take specific actions to improve your digital security.

Tactical Tech's Security-in-a-Box: Detailed chapters for practical, technical ways to increase your digital security (email, text, password management, WiFi, etc).

Electronic Frontier Foundation's Surveillance Self-Defense Toolkit



Doxxing Prevention: Managing Personally Identifiable Information online (PII)

Brightlines is a woman-owned company offering comprehensive services to proactively monitor and scrub you and your family's personal information online to prevent doxxing, data leaks and privacy violations.



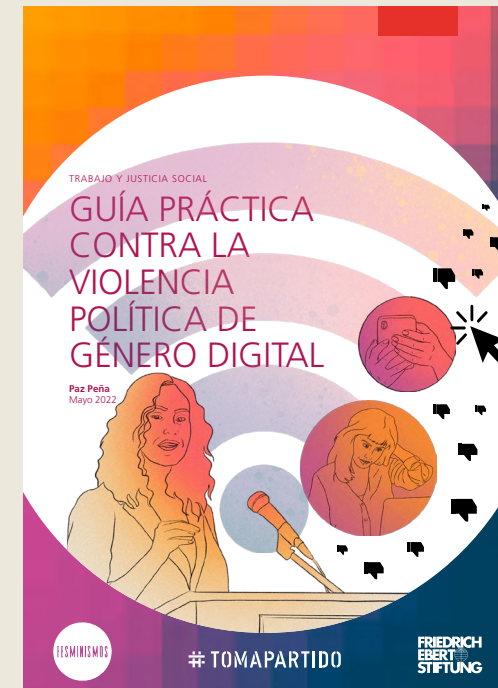


#SHEPERSISTED

Digital Resilience Toolkit for Women in Politics

Specifically designed for women in politics, this is a comprehensive and practical guide with a strong focus on communications strategies to address disinformation specifically for progressive women candidates. See “Strategies for responding” (page 23-34), real-life examples of counter speech, the section on “How to Decide Whether or Not to Respond” (page 27 & 28), and their guidance on assessing the virality (page 27-28) the “breakout scale”, a [Brookings framework](#) for assessing the reach and impact of the attack.

Includes guidance on how to address progressive issues often used by the far right to malign a candidate, such as reproductive rights and LGBTI rights, and common stereotypes disinfo content themes exploit (page 19).



#TOMAPARTIDO

Practical Guide to Confronting Digital Gender-Based Political Violence

Facing a troubling reality in Chile, where 67% of women candidates report receiving violent messages during campaigns, #TomaPartido launched a digital security guide in partnership with [Friedrich Ebert Stiftung](#) to help counter this trend. Taking a feminist lens, the guide is designed for individuals and organizations confronting digital political violence. It outlines common types of attacks and offers concrete, accessible steps to strengthen digital safety.

The guide is available in both Spanish and Portuguese.

GLITCH

Dealing with Digital Threats to Democracy: A Toolkit to Help Women in Public Life Be Safer Online

Specifically designed for women in politics, this guide offers practical tips for preventing and responding to online harassment. Glitch is a UK organization committed to ending the abuse of women and marginalized people online. Section on “Preventing Privacy Violations: Digital Self-Defense” (page 5-8), includes things like two-factor authentication, virus protection, basic digital safety training for staff, etc. This organization also promotes peer support and bystander intervention strategies - for more detail see separate toolkit [Glitch online active bystander intervention](#) for ways to respond to online abuse.



My Data or Account Has Been Compromised



Access Now: Digital Security Helpline

24/7 free support in Spanish for activists, journalists, and civil-society groups. Response time: usually under two hours; staff guide you until the incident is contained.

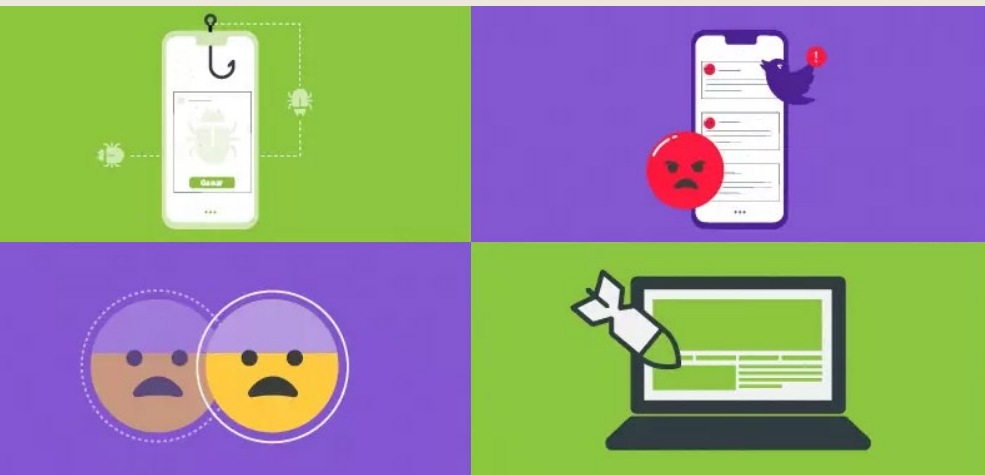
How to get help

- Email help@accessnow.org with a short summary of the problem, or
- The team does a quick risk assessment and walks you through recovery step by step.

Know the Attack: SocialTIC & Protege.LA

“Typology of Digital Attacks” (SocialTIC) shows the main ways information gets compromised—phishing, account theft, malware, impersonation, device loss, and more.

Protege.LA hosts step-by-step guides for each attack type, plus tool lists, videos, and short check-lists in Spanish.



DIGITAL FIRST AID KIT⁺

Digital First Aid Kit

Free, multilingual website (Spanish included) with interactive flows for hacked accounts, doxxing, harassment, stolen devices, and more.

Each workflow asks simple questions, then gives the exact actions and links you need—forms, platform pages, malware-scan tools.

Doxxed or Deepfake Leak



Acoso.Online Chatbot

Acoso.Online is a free Spanish-language service that helps you respond to the non-consensual sharing of intimate images and other forms of online harassment. Its Telegram bot (@AcosoOnlineBot) walks you through reporting content to platforms, checking local laws, and finding emotional or legal help. Use it when:

- Your photos or videos were posted without consent.
- You're receiving threats that private material will be leaked.
- A friend or campaign volunteer needs step-by-step guidance in Spanish.



Deep fakes and Image-based Sexual Abuse: Non consensual Intimate Image sharing, so-called “revenge porn”

Cyber Civil Rights Initiative

Has a [vetted list](#) of global organizations tackling image abuse by country who can provide legal context-specific resources and guidance.

StopNCII.org

Partners with Meta, Tiktok and other companies to block known non-consensual intimate images from being shared across platforms (for people 18 years and older). They also provide a list of [global hotlines](#) for support by region.

The National Center for Missing and Exploited Children (NCMC)

has a guide to remove explicit content of people under the age of 18 through a service called [Take It Down](#).



Preventing Image-Based Abuse with StopNCII

StopNCII.org is a global platform that helps people prevent the sharing of non-consensual intimate images online. It works by creating a digital fingerprint (hash) of the image, which is shared with major platforms like Meta and TikTok to block its upload without needing to share the image itself. The tool is free, anonymous, and available in multiple languages, offering a fast response for victims of image-based abuse.

Harassment or Disinformation Wave



Social Media Monitor Toolkit

Digital Democracy Monitor's, Social Media Monitor Toolkit, offers a step-by-step guide for understanding and doing social media monitoring in every platform.

It is a guide developed specially for electoral issues, but it can be applied to any circumstances. It approaches the importance of social media monitoring, how to build your own team, and when and how to report your findings.

Digital Democracy Monitor focuses on online political discourse, specifically information manipulation and online violence, globally.

DIGITAL SECURITY GUIDES

Foundations for protecting your information

Consumer Reports Security Planner:

Simple, comprehensive and interactive online survey “wizard” that easily helps you to design a technology-focused digital security check list and find resources specific to the tools you use in your context (i.e. windows vs. Apple, messaging apps, etc.).

Pen America’s Online Harassment Field

Manual: Available in English, French, Spanish, Arabic and Swahili, this comprehensive, holistic and approachable resource offers guidance for before, during and after online attacks. Specifically, see their guide to [assessing the physical risk of an online attack](#) and their guidelines for [safely practicing counterspeech](#).



DOCUMENTING ONLINE ATTACKS

Monitoring trends and building evidence for egregious cases

Glitch offer an [online abuse documentation spreadsheet](#) you can copy to systematically track and organize incidents of online harassment.

Without My Consent: Guide for digital [evidence preservation](#).

Online SOS: Guidance on how to [document](#) online harassment.

The logo for 'Glitch' is displayed in a bold, white, italicized sans-serif font. It is centered within a solid blue rectangular background.

The International Foundation for Electoral Systems' (IFES) Crisis Communication and Combatting Disinformation: Playbook Template for Electoral Management

Bodies outlines approaches for effective strategies, responses and processes to address disinformation. This includes scenario planning, creating a Disinformation Response Team or Processes, developing template statements to likely disinfo, etc. While this resource is focused on government institutions (Electoral Management Bodies), many of the recommendations are applicable or can be adapted for individual leaders in politics, as disinfo about government institutions often feeds on similar fears and stereotypes.

- See Checklists for Incident Preparation and Rapid Response, which summarize recommended actions for what to do before, during and after an event (page 20-22).
- See good communication practices for countering disinformation (page 7-9), including speaking clearly and plainly, leading with facts, not repeating disinfo, making your content visual.
- Stakeholder outreach, mapping and proactive relationship management (page 12) should include civil society organizations, academia, media, advocacy, government officials, political opponents, respected legal experts, former government officials and other affiliations.

Legal or Emotional Support

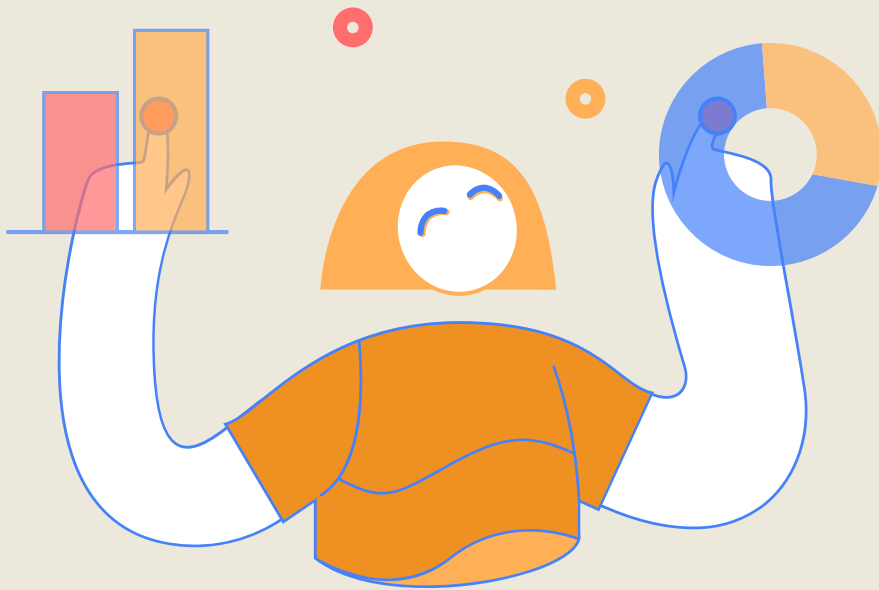


PEN America's report, [The Power of Peer Support: Helping Journalists Persevere in the Face of Online Abuse](#), provides an overview of relevant peer support models and methods.

While specifically addressing journalists, this resource crosses over well to women in politics who also experience online harassment as an occupational hazard, and also may have varying levels of institutional support.

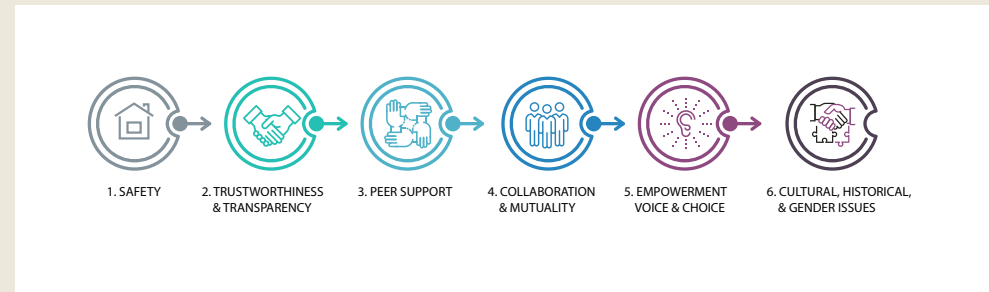
Also, check out their Online Harassment Field Manual for this section, "[Guidelines for how to talk to friends and allies.](#)"

PEN America focuses on global freedom of expression, specifically supporting journalists has been supporting journalists in the U.S. and globally for over 100 years.



This [Self-Care Assessment](#) is a simple and practical one-page survey you can do anytime to examine your own physical, psychological, emotional, spiritual, workplace and professional needs.

It is designed to measure how well you are balancing your own needs with the needs of those you serve. It is recommended you re-assess yourself on a regular basis and use the results to create or adapt a Self-Care Plan as needed. It is designed to be used as a tool to help you gain awareness about your own needs and limitations, maintain balance between your work self and personal self, and deepen your connection to this work.



This infographic offers [Six Guiding Principles to a Trauma-Informed Approach](#) for organizations and teams.

These principles, such as safety, transparency, peer support and collaboration can guide how an organization or team works to improve the impact of the services it provides. Developed for a public health audience, but widely applicable across sectors.

[Vicarious Trauma: A Trauma Shared](#) - This short article provides information about what vicarious or secondary trauma is, how it can affect you, and three practical ways to address it through exercise, reorienting or redirecting our focus, and cultivating other healthy practices like meditation and breathing. Vicarious trauma happens when exposure to second-hand traumatic material affects us negatively.

- [Acoso Online Emergency Line](#) (Regional, Spanish)
- [Vita-Activia Help Line](#) (Global, Spanish and English)
- [Maria D’Ajuda Help Line](#) (Brazil, Portuguese)
- [SOS Digital Support Line](#) (Bolivia, Spanish)
- [AccessNow Digital Security Help Line](#) (Global, many languages)

Social Media Company and Cell Phone Guides

Help Desk Directories offered by Tech Companies provide information on how to manage your account privacy and preferences using built in features such as two-factor authentication (2FA), reporting, blocking, muting, or account delegation, which gives a trusted person or team member direct access to the account, and is useful to monitor and document abuse.

Some companies also provide specific guides for women, politicians, and charitable organizations.

CELL PHONE GUIDES

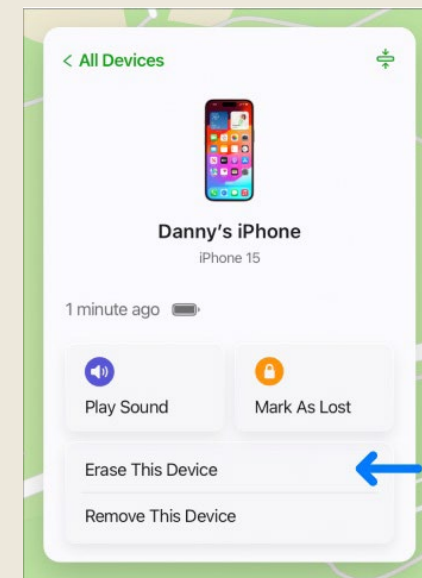
Remote Wiping of Data

Remotely wiping information from a lost or stolen device is essential to ensure accounts and sensitive information are secure and are not taken over by malicious actors.

Mobile operating systems like Apple/iOS and Google/Pixel/Android offer the ability to wipe your phone remotely should it become lost or stolen.

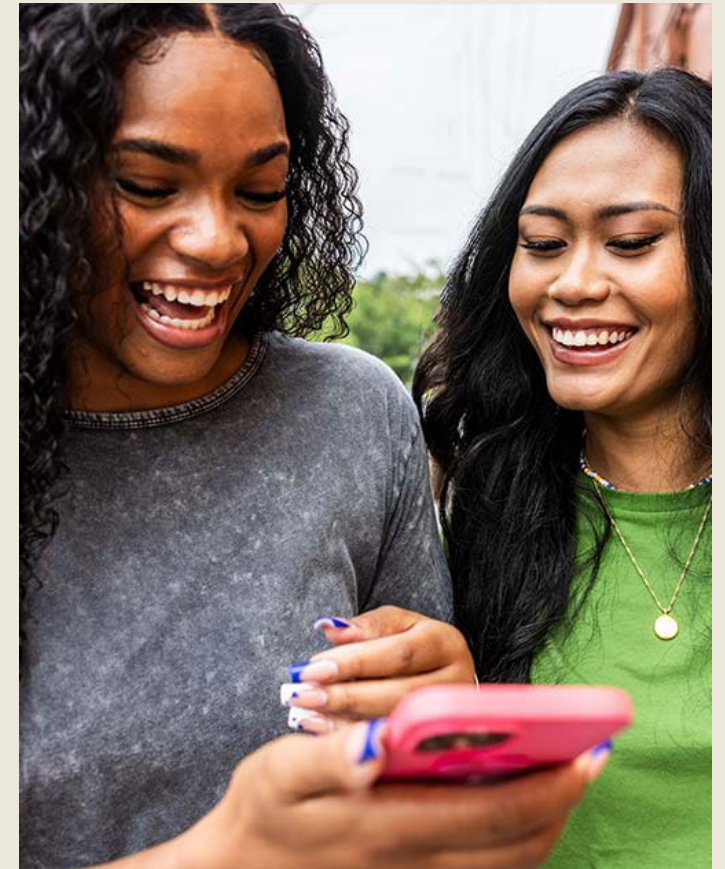
See [Apple Guide](#) and [Google/Android Guide](#).

Available in different languages.



META

Tools to Secure and Protect Accounts on Facebook, Instagram, WhatsApp, Messenger



- [Meta Safety Guide For Women in Politics](#)
- [Meta Government and Nonprofit Resource Center](#)
- [Meta Government and Nonprofit Guide to Security Best Practices](#)
- [Meta Election Center: European Parliament](#)

Available in different languages.

Social Media: Guides to Reporting, Blocking or Restricting Content

Note: Please double check country-level laws that may restrict the accounts of elected officials from blocking constituents or limiting comments.

GOOGLE

- [Google Help Center & Gmail account delegation](#)
- [Removal request for NCII](#)
You or an authorized representative can submit a request to remove links to the content from Google search results.

FACEBOOK

- [Reporting Harmful Content](#)
- [Not Without My Consent, Facebook Safety Center](#)
- [Stop Sextortion Hub](#)
- [Blocking](#)
- [Account delegation](#)
Gives a trusted person or team member direct access to the account, useful to monitor and document abuse

INSTAGRAM

- [Reporting on Instagram](#)
- [Safety Center and Account Delegation](#)
- [Instagram's guide to blocking](#)

LINKEDIN

- [Report Inappropriate Content, Messages, or Safety Concerns](#)
- [Safety Center and Account Delegation](#)

TIKTOK

- [Report a Problem](#)
- [Safety Center](#)
- [Bullying Prevention Guide](#)
- [Well-Being Guide](#)

X/TWITTER

- [Twitter Safety Center and Account Delegation](#)
- [Twitter/X's guide to blocking and muting](#)

WHATSAPP

- [Help Center](#)
- [Blocking and Reporting Contacts](#)

YOUTUBE

- [YouTube Help Center](#)
- [YouTube Commitment to Managing Harmful Content](#)
- [Reporting inappropriate content](#)

When something is reported on YouTube, it is automatically taken down, sometimes with additional reviews on the backend. You can report videos, playlists, thumbnails, links, comments, live chats, channels, and ads.



Deep-Dive Library

Why it's here and how to use it

Welcome to the reference room. When the urgent fires are out, come here to learn the why behind every checklist step. You'll find longer reports, case studies, legal explainers, and mental-health resources—everything that adds depth and evidence to the quick-action sections. Use it to train your team, design workshops, or answer those “where's the data?” questions from partners and the press.

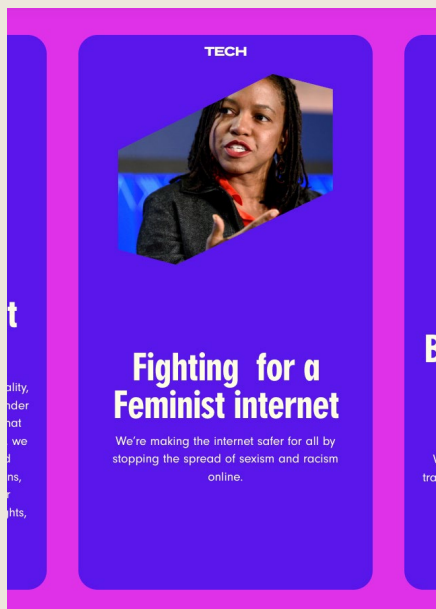
Applied Research to Understand Online Abuse & Harassment



Women's Media Center: Online Abuse 101

The first step to combating online abuse is developing a shared language to identify and describe it. Women's Media Center created the "Online Abuse Wheel," a foundational educational advocacy tool for understanding online abuse and its impacts. It provides practical definitions of online abuse, details over 25 common tactics used by perpetrators, and includes a Frequently Asked Questions (FAQ) section useful for educating staff and stakeholders, as well as informing communication strategies.

Inspired by the original "Power and Control Wheel" from the Duluth Model on Domestic Violence. For more terms and definitions of different types of online abuse, see also PenAmerica's Online Harassment Field Manual's Glossary of Terms.



UltraViolet: Reporting in an Era of Disinformation: Fairness Guide for Covering Women and People of Color in Politics

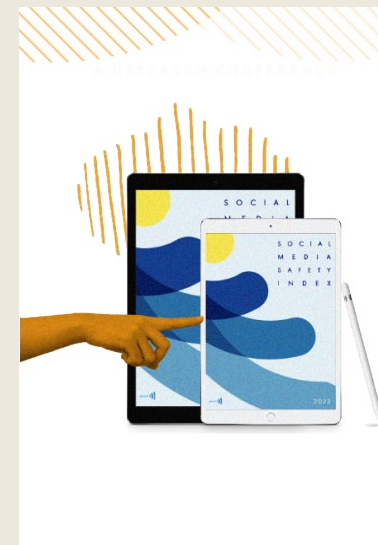
Provides specific examples of real headlines using common sexist and racist tropes or stereotypes in the media. Useful for educating staff and stakeholders to formulate communication responses, reframe an attack and redirect it from you. Written primarily for a journalist audience.



Digital Security: Tech Support to Prevent Online Attacks

Coalition Against Online Violence: The CAOV 2024 Mapping Report

The report provides strategies for response and prevention, especially guidance on peer support networks (starting page 18). Emphasizes direct access to peer support, developing resource lists/orgs who can support, and creating action plans before being attacked. Audience focus is journalists.



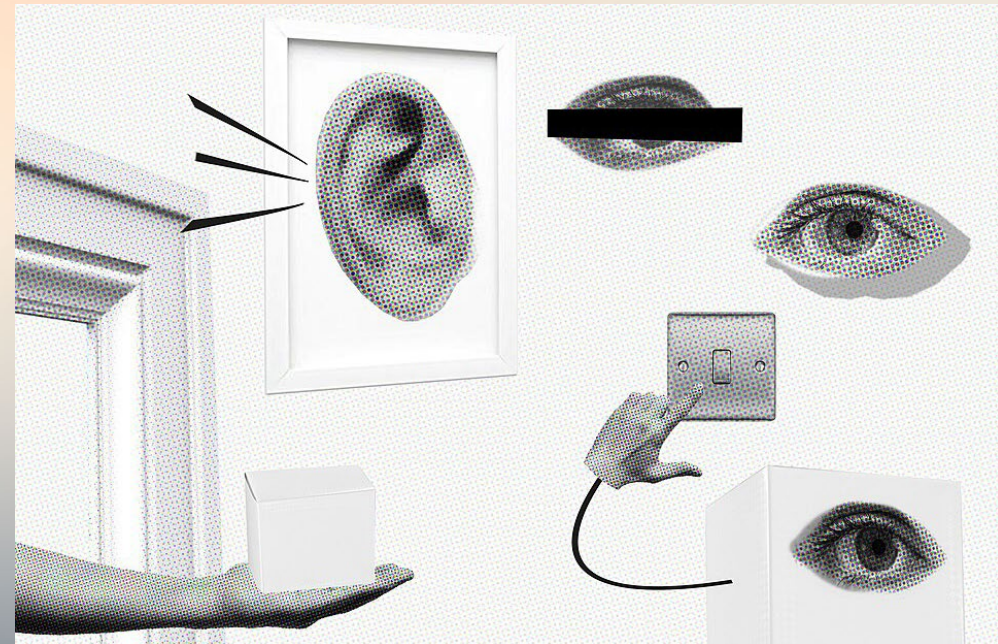
Security In-A-Box: Create and Maintain Safe Passwords

Step-by-step tips on making and storing tough passwords, turning on two-factor logins, and seeing whether your credentials have leaked.

School of Activism: Safe Passwords

The Brazilian organization dove in the safe password multiverse: they have [a diagram for you to go through and check if your password is safe](#), [a step-by-step guide to check if your password has ever been leaked](#) and even some fictional (or not) [stories about passcodes](#), changing and creating them. Have a good read!

Available in Portuguese.



Disinformation Tools & Response Strategies for Women in Politics

Mujeres Libres en Política (Women Free in Politics)

This guide is published by the Organo Electoral Plurinacional and the Supremo Tribunal Federal of Bolivia - aims to help women in politics identify online harassment and political violence, strengthen their capacity to defend themselves against digital attacks, and build knowledge to recognize different forms of violence, understand how to report them, and access the tools needed to support and strengthen women's political participation both online and offline.

Available in Spanish.



DEMOS

Engendering Hate Report

This report uses in-depth research in Poland and the Philippines to investigate the rules that state-aligned actors employ in their gendered disinfo attacks on women in public life or elected office (Chapter 4).

These “rules” stem from pervasive misogynistic stereotypes that seek to prove that women are devious, stupid, and unfit for politics, seek to make them too afraid to talk back, praise women for being sexy but condemn them for being sexual, prove that strong men must save women, and demonize the values women hold. Chapter 5 provides counter speech examples and themes.

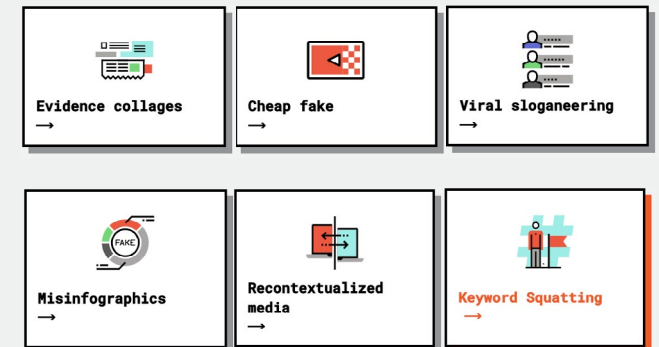
DEMOS

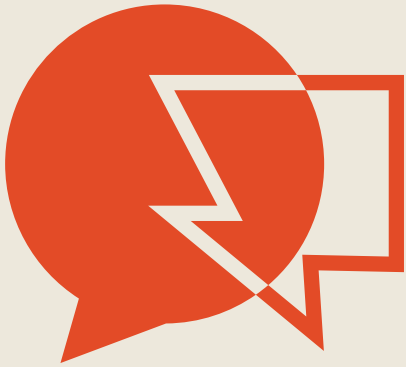
Applied Research to Understand Online Abuse & Harassment

The Media Manipulation Casebook

With a focus on mis & disinformation tactics, common media manipulation tactics are defined and explained. It highlights common ways disinfo campaign operators take advantage of our networked media ecosystem.

Explainers cover cheap fakes, misinfographics, recontextualized media, viral sloganeering, and keyword squatting.





Dangerous Speech Project: A Practical Guide to Dangerous Speech & Counterspeech

The Dangerous Speech Project defines dangerous speech as any form of expression (e.g. speech, text, or images) that can increase the risk that its audience will condone or participate in violence against members of another group. This resource provides an analysis and breakdown of the different elements of rhetoric more likely to become violent, as well as an overview of counterspeech.

The effectiveness of counterspeech depends on the goal of the counterspeech- and is often difficult to measure. Goals can range from changing the attitude of the perpetrator to limiting the reach of the harmful content to providing the subject of an attack with supportive messages.

#NotTheCost: Violence Against Women in Politics

The National Democratic Institute explores the hallmarks of gendered threats and violence against women leaders in democratic politics over a five year period, emphasizing awareness raising and institutional response tactics.

They emphasize that while political violence happens against both men and women, violence against women in politics targets women because they are women, in ways that apply particularly to women (e.g. sexual violence and sexist attacks), and discourages all women from political activity, with a particularly negative impact on young women or new entrants to politics.

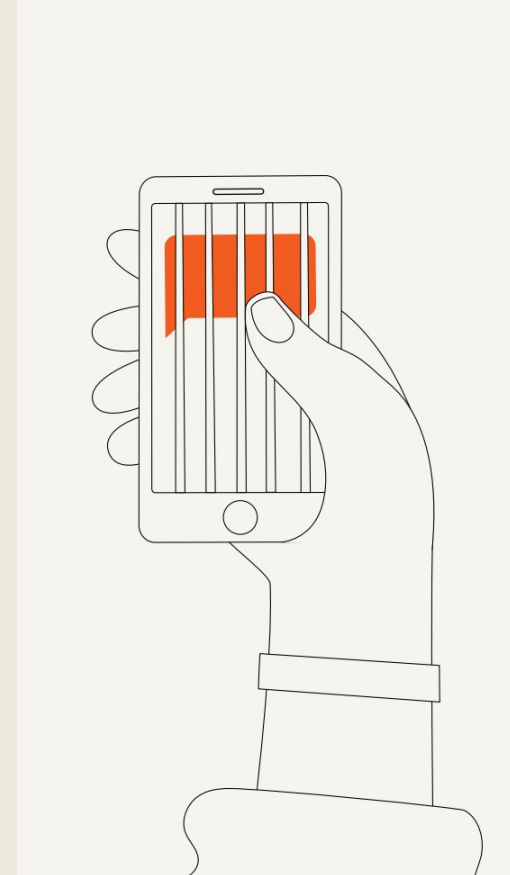


MonitorA

Created by [AzMina](#) and [InternetLab](#) during Brazil's 2020 elections, this project tracks online political violence. It revealed that women, Black, LGBTQIAP+ people, and older people are often attacked for their identities. In 2022, with new laws on gendered political violence, it expanded its scope. Available in English and Portuguese.

In 2023, coLAB at UFF launched [a map showing the intensity and forms of gender-based political violence on Twitter, Facebook, Instagram, and YouTube](#).

Likewise, in Colombia, [Fundación Karisma](#) has been doing [research to define digital violence against women politicians](#) (available in Spanish) in the country and understand its consequences for their work and life.



Gendered Online Violence Against Women in the Public Eye

In 2022, the Alianza Regional conducted a qualitative study on online gender-based violence against women with a public voice in Latin America, highlighting its impact on freedom of expression. The report documents cases from 15 countries, including Argentina, Brazil, Colombia, Mexico, and Venezuela, showing how digital attacks seek to silence women in politics, journalism, activism, and other public roles.

Available in Spanish.





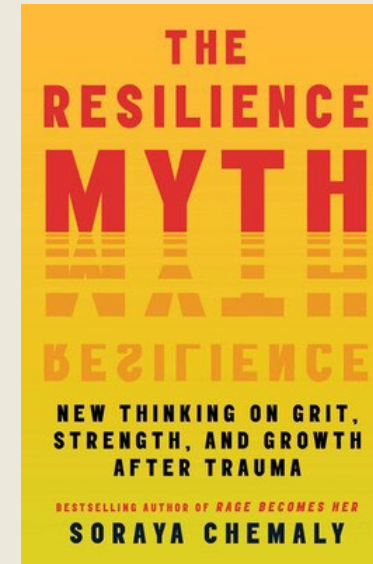
Gender-based Political Violence in the Digital Sphere in Latin America

The document explores the issue of gender-based political violence in the digital sphere against women in Latin America.

Despite progress in women's political representation in the region, significant challenges remain—especially gender-based violence in politics. This research examines how new technologies have enabled emerging forms of violence targeting women in politics. It systematizes key concepts and case studies, introducing a “pyramid of digital political violence” that shows how different forms of harassment can escalate to physical violence. It also reviews regional legislation on digital political violence and concludes with urgent recommendations for all relevant stakeholders.

Available in Spanish.

Legal or Emotional Support

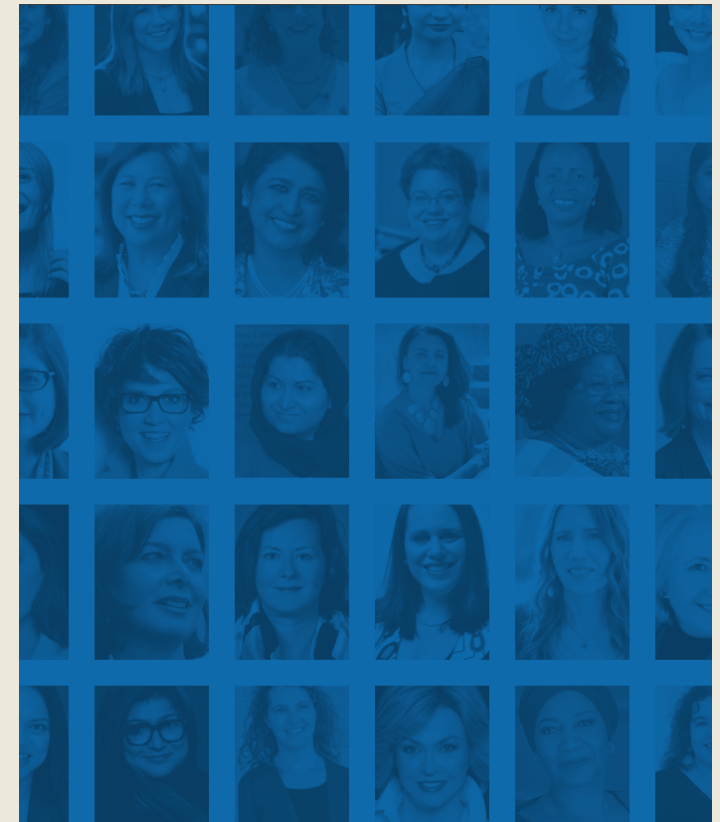


The Resilience Myth: New Thinking on Grit, Strength, and Growth After Trauma

Author Soraya Chemaly challenges us to adapt our thinking about how we survive in a world of sustained, overlapping crises, by pivoting away from narratives of self-reliance, mental fortitude, and positivity toward truly sustaining interdependence and nurturing relationships. Based on comprehensive research and eye-opening examples from real-life, she offers alternative visions of relational hardiness by emphasizing care for others and our environments above all.

Soraya Chemaly is an award-winning feminist writer whose work focuses on the role of gender in culture, politics, religion, and media. She is the Director of the Women's Media Center Speech Project and an advocate for women's freedom of expression and expanded civic and political engagement.

Case Studies by Country or Region



GLOBAL CASE STUDY

#ShePersisted: Women, Politics and Power in the New Media World

Short, practical advice from women in politics, based on interviews with over 85 women leaders, including former Prime Ministers, one former president, civil society, television, journalism and technology leaders. Includes a desk review of over 100 publications. See “How Women Politicians Can Use Traditional and Social Media to Succeed” (page 54) and (page 22-27).

COLOMBIAN CASE STUDY

Francia Márquez: Disinformation Narratives During the Campaign

A detailed report by [Colombiacheck](#) on disinformation narratives targeting then-vice-presidential candidate Francia Márquez, highlighting how sexist, racist, and classist tropes—like calling her a guerrillera, corrupt contractor, or witch—were used to undermine her legitimacy.

Available in Spanish.

COLOMBIAN CASE STUDY

Alerta Machitroll: Using Humour to Tackle Gender Violence Online

Campaign by [Fundación Karisma](#) launched during the 16 Days of Activism (2015). Aimed at online misogynistic discourse, the initiative used digital badges (“incurable machitroll” / “redeemable”) to denounce and satirize sexist comments in public forums — generating lasting impact on awareness and digital culture. It is also a [successful case of counterspeech](#).

Available in English and Spanish.





MEXICAN CASE STUDY

Senator Andrea Chávez: Responds to AI-Based Digital Violence

In 2024, Mexican Senator Andrea Chávez was targeted with an AI-generated fake image showing her in a sexualized context. The image, shared by a political cartoonist, aimed to humiliate her. She publicly condemned the attack and filed a legal complaint under Mexico's Ley Olimpia, which penalizes non-consensual intimate content. Her response sparked national debate on digital gender-based violence and the urgent need to regulate AI misuse in political contexts.

Available in Spanish.

Understanding the Problem

Online abuse is intricately connected to our offline realities, and understanding it better can inform strategies to prevent and address it.

Naming the types of attacks and patterns assist in evaluating risks and determining actions to take. One of the first steps to combating online abuse is developing a shared language to identify and describe it. Applied research and case studies can offer context-based background applicable across regions.

Overall, it is important to remember the broader implications of online abuse. Primarily, it seeks to amplify existing social biases in order to disenfranchise women and underrepresented people from participation in government and in civic life. The common denominator of the most recurring disinfo campaign narratives is fear that life as one knows it will take a turn for the worse between the erosion of values, sovereignty, and purchasing power.

Definitions and Examples

Online abuse and harassment

Online abuse and harassment has broad definitions that include a wide range of attacks leveraging social anxiety and fear of “the other,” fueled by sexism, racism, ableism, religious prejudice, homophobia and transphobia. It can include many types of abuse involving hate speech, impersonation, disinformation campaigns, manipulation of images or non-consensual sharing of personal information, and doxxing, all of which can impact a person’s offline life.

Doxxing

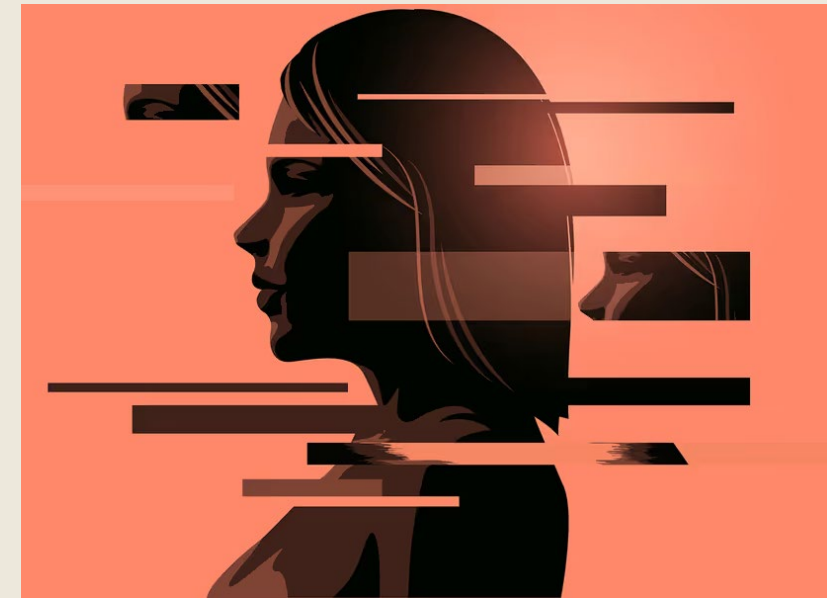
Doxxing is the unauthorized retrieval and centralized publishing of personal information such as addresses, phone numbers, emails, names of family members or children. It can cause fear and chill the speech and actions of women political figures through veiled or explicit suggestions of offline violence.



Misinformation and Disinformation

While misinformation and disinformation are often used interchangeably, generally misinformation is the inadvertent spread of false information without intent to harm, while disinformation is false information designed to mislead others, deliberately spread with the intent to confuse fact and fiction. Typically, it is highly emotive, focused on values, and visually compelling to prompt reactive sharing.

Disinformation campaigns and bad actors, including States, can utilize media manipulation, trolls and bots to distort, exaggerate, and amplify their messages. In doing so, the disinformation creates an illusion of widespread disapproval in an attempt to discredit a candidate, drown out opposition, create sympathy for their cause, or change what information is seen by others.



For women in politics, traditional gendered stereotypes, norms, and gender roles are weaponized to elicit fear and reinforce the historical dominance and power of heterosexual men in politics and broader society.

These campaigns seek to spread false information about their targets by co-opting existing values and stereotypes and inflaming people's emotions.

Impact and Societal Costs

The persistence of online attacks against women in politics can undermine broader democratic processes and values.

Women are underrepresented in elected office; only 27.1% of Members of Parliament globally are women. Despite that, women face outsized online attacks, often because they are seen as disrupting the status quo of political power traditionally held by men. Leading global, multilateral institutions such as the United Nations, the Inter-Parliamentary Union, the Council of Europe and Organization for American States all explicitly recognize that, when compared to their counterparts, women in politics experience heightened threats and attacks spanning the offline and online continuum at greater scale, intensity, and severity.

Disinformation can not only devalue and delegitimize the credibility of individual women leaders, but it can more broadly disenfranchise women and underrepresented people, including girls, from participation in government and in civic life. These attacks are compounded for women facing intersectional discrimination and bias on the basis of race, disability, ethnicity, religion and sexual orientation.

Gendered disinformation compromises both the free expression of politicians and their constituents. Gendered disinformation and online attacks undermine the functioning of a free and fair democracy and exploit public distrust of government and negative sentiments such as rage and fear to polarize and mobilize the audience, therefore it is crucial to acknowledge and address public distrust to heal democracies.

**Produced for the
2024 Fellowship**

**Written and researched by
Betsy Bramon**

**Updated for the
2025 Fellowship by
Alejandra Parra and
Gabriela Juns**

**For a digital version
of this guide**



FIELD

A home ground
for visionary
political leaders

