#SHE PERSISTED

A Digital Resilience Toolkit for Women In Politics

Persisting and Fighting Back Against Misogyny and Digital Platforms' Failures

Kristina Wilfore

#ShePersisted is committed to tackling gendered disinformation against women in politics. We research digital harms, support women leaders to build digital resilience and advocate for improved digital standards. Learn more here.

INTRODUCTION

Women in public leadership positions or candidates for office face unprecedented levels of online violence and abuse. At #ShePersisted, we are often asked, "What can women do to protect themselves?"

The answer is unsatisfying. In reality, with the lack of accountability of digital media platforms to safeguard women against online harms, there is very little action women who are targeted can take to guarantee protection. Furthermore, asking women to bear the burden of protecting themselves - in light of this fundamental lack of accountability and transparency of social media platforms - risks turning attention away from the way that technology, and the choices of large platforms, makes the problem worse.

As a result, we must start from the recognition that the spread of online hate can be largely attributed to the failures of social media platforms to protect women on their platforms, **prioritizing profit** over the safety of their users. As long as the platforms continue to actively monetize harm to women users on their platforms, individual leaders taking steps to protect themselves online can never truly fix the issue, or completely protect themselves. We cannot ease up on pressuring the platforms to take meaningful action. We must continue to push for more transparency and accountability.

Through the research #ShePersisted has conducted over the last two years, we notice some disturbing trends. Women are either silencing themselves online, or second-guessing a career in public activism or higher office. Gender-based violence online and gendered disinformation campaigns are having a tangible impact on discouraging women to run for office or pursue leadership roles, with devastating consequences on **democracy**, national security and **social norms**.

We have been asked time and time again to create a guide outlining the steps that individual women can take to lessen the harms that they face online. Even though we were hesitant to remove the burden off of the platforms, we recognize that this is a crisis that cannot only wait for platforms to take action. In response to the stopgap emergency at hand, we created this guide to outline certain steps that can help women pursuing a leadership position and/or if we find ourselves the target of online abuse.

METHODOLOGY

There is a great deal of existing literature speaking to various forms of security and online protection. After reviewing dozens of existing guides, attending various trainings and sessions, and talking with women leaders in our network, we have created a crowdsourced guide specifically aimed at advice for women leaders in the public eye. Aside from the advice laid forth, we are including links to further resources for existing guides, trainings, and direct support.

ACKNOWLEDGEMENTS

#ShePersisted is incredibly lucky to work in a space filled with innovative and endlessly generous individuals who are open to sharing their expertise in responding to digital harms. These are vital partnerships that contribute to the wellspring of support and information regarding women's rights and digital rights from which this toolkit has drawn. We are grateful for their contributions, both tacit and direct, from a great many of these activists, experts, and organizations without whom this toolkit could not have been made. The following is a long but by no means exhaustive list of organizations we have drawn from, and those people we would like to directly thank for their invaluable help in creating this resource.

INDIVIDUALS

This toolkit would not have been possible without the research, testimony, and direct contribution of a number of individuals, whom I would like to personally thank. Myself and #**ShePersisted's** co-founder Lucina Di Meco are endlessly grateful for the engagement and input from key allies who generously contributed quotes that fundamentally shaped this toolkit's message.

Thank you very much to Natalia Mori, A'shanti F. Gholar, Vanessa Cardenas, Abbie Hodgson, Dahae Sue and Julia Gillard, Sara Guillermo, Valeria Fedeli, Ágnes Vadai, Manira Alva, Celinda Lake, Sonja Lokar, Rumbidzai Chisenga, and Mae Dobbs. I have drawn on the work of researchers Safiya Noble, Anat Shenker-Osorio, Kelsey Suter, Jiore Craig, Rebekah Tromble, Ben Nimmo, and testimony from Ghanaian MP Comfort Doyoe Cudjoe-Ghanash, former Canadian journalist Tamara Taggart, Ukrainian journalist Olga Rudenko, former Canadian Minister of Environment and Climate Catherine McKenna, first Lady of Namibia Monica Geingos and Colorado State Senator Rhonda Fields. Lastly, this toolkit was put together with help from our program associates at **#ShePersisted**, Imogen Learmonth and Sarah Hesterman, and former program associate Alcy Stiepock MacKay,

ORGANIZATIONS

Amnesty International, Barbara Lee Family Foundation, Center for Countering Digital Hate (CCDH), Centre for Feminist Foreign Policy (CFFP), COACH Community, Mentoring, Community Change, CREA, Cyberwomen, Dewey Square Group, Electronic Frontier Foundation, End Violence Against Women Coalition, Fair Fight, Free Press Unlimited, Glitch, GQR, HateAid, HeartMob, International Foundation for Electoral Systems (IFES), International Women's Media Foundation (IWMF, Knight Center for Journalism in the Americas at the University of Texas at Austin, Media Matters for America, NARAL Pro-Choice America, National Coalition Against Domestic Violence (NCADV), Observatory on the Universality of Rights (OURs), Ontheline Platform for Newsrooms, Over Zero, PEN America, Right To Be, Rory Peck Trust, Safe Sisters, TrollBusters, UltraViolet, Women's Legal Education & Action Fund (LEAF)

WHO IS THIS GUIDE FOR?

This toolkit brings together existing resources for digital security and tactics for preventing and handling online harms. It targets advice specifically for women elected leaders, activists, election consultants working with women's campaigns, journalists, and the broader international women's community.

CONTENTS

This guide is broken into three main sections

A #ShePersisted Perspective on Online Abuse

Framing the Problem

To date, social media platforms have allowed online attacks against women in politics and journalism to scale and become sources of revenue. Despite refusing accountability, platform algorithms are designed to prioritize disseminating content with greater engagement potential—regardless of whether it is truthful, or irrespective of harm or social impact. Revenue grows when already outrageous and sensationalistic posts get further amplified by coordinated campaigns—whether they are carried out by authentic or inauthentic actors. Reform to protect women online and encourage women's political engagement requires increased platform transparency and accountability, as well as the need for a **new digital social contract.**

For women already in political office, it is essential to understand the incentive structure that allows for this type of content to thrive, and devise regulatory mechanisms for social media platforms that establish better standards for consumers.

The Role of Government

Even while recognizing private companies' purview to determine their own business model, governments can create regulatory frameworks that set the stage for better social media standards. Efforts to encourage technology companies to change their products and practices to reduce harm is an enormous undertaking against a powerful, largely unregulated industry. It is essential that those reform efforts move forward with a more diverse set of countries, and are informed by the experience of women and the growing knowledge of how gendered disinformation manifests itself.

As governments around the world consider reforms to technology oversight—such as establishing a "duty of care" as is being discussed in the United Kingdom and the European Union's Digital Services Act to increase transparency and risk requirements—addressing gendered disinformation must be a bigger part of the policy agenda aimed at reducing online harms. A recent campaign from #ShePersisted demanded that digital platforms take decisive actions to reduce online gender-based violence on their platforms. We produced this **video** showcasing the harms to women politicians and journalists and our efforts were featured in **Politico**. As a result of the action of allies and civil society organizations, the article of the DSA that necessitates risk assessments for very large online platforms now explicitly includes a risk assessment for the "right to gender equality."

Women in politics are the targets of overwhelming volumes of gendered disinformation and online abuse in the forms of fake stories, humiliating or sexually charged images

The Threat to Women Leaders

Women in politics are the targets of overwhelming volumes of gendered disinformation and online abuse in the forms of fake stories, humiliating or sexually charged images, including photomontages and deepfakes, often aimed at framing them as untrustworthy, unintelligent, and uncontrollable (emotional/angry/crazy). Sexualized attacks are also a constant backdrop to disinformation aimed at women,

relying on sexist tropes that women are weak and incompetent and not fit for pubilc office. Overall, these attacks are designed to alter public understanding of female identifying politicians' track records to undermine and marginalize them, as well as to discourage women seeking political careers.

Women in leadership already face heightened and unfair expectations for qualifications, likeability, trustworthiness, intelligence, appearance, and expectations of sexuality. Having attacks on these gendered themes amplified and spread on online platforms adds a new barrier to women's political involvement. Unprecedented levels of online abuse have recently proven to discourage women from running for office or remaining in the public eye.

The Threat to Democracy

As well as having devastating consequences for the women they target, online attacks against women in politics not only reflect but can also change social norms and behavior. Through social media, misogynistic language and narratives that had been latent in society find new strength, to the point of weakening social norms of inclusion and civil discourse, and normalizing abuse and impunity for its perpetrators.

While sexist attitudes are integral to understanding violent extremism and political violence, social norms per se don't explain how attacks against women in politics have been weaponized for political gain and cynically coordinated by illiberal actors that take advantage of algorithmic designs and business models that incentivize fake and outrageous content. A new wave of authoritarian leaders and illiberal actors around the world use gendered disinformation and online abuse to push back against the progress made on women's and minority rights. This movement seeks to push women politicians and activists aside, reignite gender stereotypes and misogyny, and strategically take advantage of technology as a tool in these campaigns to attack women in politics, aggressively challenge feminism, and attack liberal values. State-aligned gendered disinformation campaigns are used as a deliberate tactic to smother opposition voices, erode democratic processes, and silence demands for government accountability.

Online attacks against women in politics not only reflect but can also change social norms and behavior.

Harm Mitigation as a Stopgap Emergency

Despite all of this, the platforms continue to fail to take meaningful action and keep putting women using their channels at risk. Pressure needs to stay consistently on the platforms for true change, but in the meantime women are left to fend for themselves and take personal steps to mitigate harm online and protect themselves to the greatest degree possible from online abuse.

Below we'll walk you through that process, beginning with preemptively enhancing your digital security through reporting then documenting and responding to attacks online, while obtaining the necessary technical and psychological support throughout.

Glossary

Misinformation

False or misleading information that was not purposefully created or spread with intent to harm, but can nevertheless lead to harm.

Disinformation

Purposefully false or misleading information created and spread with the intent of doing harm.

Gendered Disinformation

Gendered disinformation is the spread of deceptive or inaccurate information and images against women political leaders, journalists, and women public figures.

Following story lines that draw on misogyny, and gendered stereotypes, the goal of these attacks is to frame women politicians and public officials as inherently untrustworthy, unintelligent, unlikable, or uncontrollable – too emotional to hold office or participate in democratic politics.

Building on sexist narratives and characterized by malign intent and coordination, gendered disinformation both distorts the public understanding of women leaders' track records and discourages women from seeking careers in the public eye.

Online gendered abuse

Online gendered abuse refers to a spectrum of activities and behaviors that involve technology as a central aspect of perpetuating violence, abuse, or harassment against (both cis and trans) women.

How technology is used as a form of abuse

The ways and means misogynistic actors can use to target women online are as plentiful as the types of digital communication available to us. However, this type of abuse, especially if it is coordinated, can fall into identifiable patterns. A noticeable upswing of this type of activity on your social media accounts is often a telltale sign of a targeted hate campaign or coordinated abuse.

According to the **Women's Legal Education and Action Fund** (LEAF) and informed by additional research, activities that fall under the umbrella of gender-based online abuse include:

"The tone and frequency of online attacks make them difficult to ignore or dismiss. Rather than letting them drain your power, harness them. Know that by continuing to bravely do your work, you're exercising your right to exist in political spaces and will be able to enact policies and practices to combat the attacks, ensuring other women are protected from sex-based violence and vitriol."

Abbie Hodgson, USA,
Director of The Ascend Fund

Doxxing
(publishing and disseminating private information, like your home address)

Online mobbing
(a large number of people simultaneously engaged in online harassment or online abuse against a single individual)

Sextortion
(extorting someone online through threats to share sexual information, images or clips of an individual unless they pay the perpetrator, follow their orders, or commit sexual acts with or for them)

Trolling
(deliberate inflammatory, insincere, digressive, extraneous, or off-topic direct messaging, or posting about an individual in a public forum)

Sexual exploitation resulting from online luring (grooming young women or girls through social media and various chat platforms, or posting false advertisements online, in order to lure them into 'offline' forms of sexual exploitation)

Non-consensual sharing of intimate images

Voyeurism
(surreptitiously observing or recording someone while they are in a situation that gives rise to a reasonable expectation of privacy)

Defamation
(lying about or misrepresenting an individual online to ruin their reputation and relationships)

Spying and monitoring through account hacking or interception of private communications

Threats and intimidation
(including rape threats, death threats, or threats to harm the targeted person's family and friends)

Coordinated flagging campaigns
(gaming a platform's mechanisms for reporting abuse)

Stalking
(continued unwanted contact or following of an individual through their online activity; this can often translate into in-person stalking)

Image-based abuse (including both 'deepfakes' and 'shallow fakes'. Deepfakes involve the use of artificial intelligence to produce videos that include false but realistic images of an individual. Shallow or 'cheap' fakes are videos, images, or audio recordings manipulated without artificial intelligence, such as through Photoshop or basic video editing software)

The Need for Accountability

Some of these activities may meet the threshold of illegality in certain places. Most countries have laws against things like impersonation, defamation or criminal harassment. However, there is typically a high legal threshold for proving illicit online abuse (as women's rights NGOs have **pointed out**, 'proof of intent' is a prohibitive legal minimum for prosecuting image-based abuse in the framework of the UK's new Online Safety Bill).

The vast majority of these activities are permitted online expression almost everywhere in the world, even if incessantly engaged over a long period of time. In the US, stringent first-amendment obligations mean that most online abuse is protected speech. It is precisely because so much online abuse is 'awful but lawful' that gendered disinformation can operate as a 'death by a thousand cuts' to women's safety online, and to our equal and fair democratic participation.

Though platforms are free to impose their own content policies preventing gendered online abuse, they unanimously and spectacularly fail to do so. **Recommendation algorithms** on many platforms are criticized for amplifying racist, conspiracist, and misogynistic content. Facebook and Twitter have a history of aiding **intimate partner violence**, and failing to respond to **gender-abuse reports** from women, and image-based sites like Instagram **disastrously intensify** body-image related abuse and harassment as well as

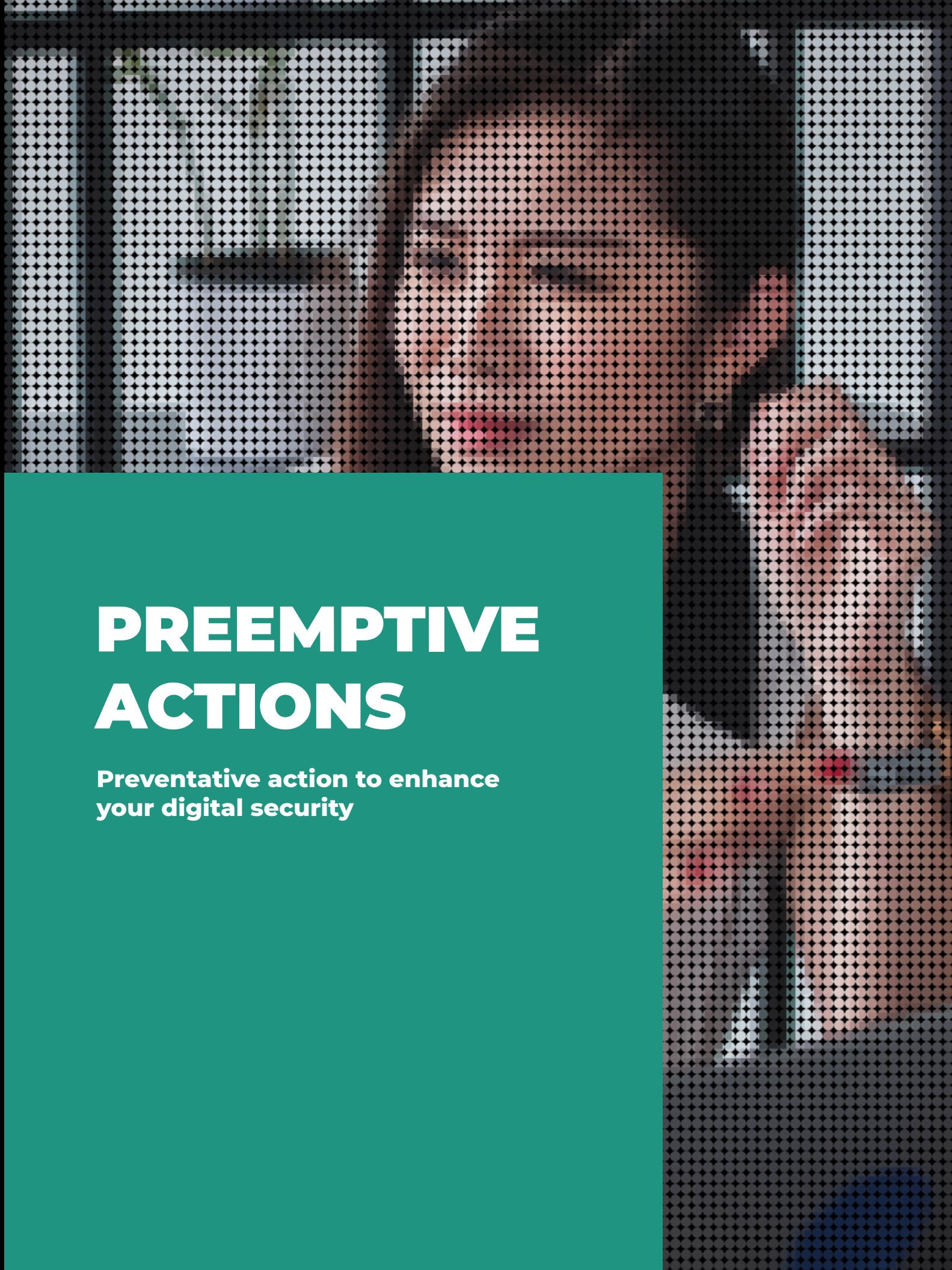
ultraviolet

non-consensual sharing of intimate images. According to the **Social Media Fails Women 'Report Card'** created by **UltraViolet**, no platform has effective, or even sufficient, policies to tackle online misogynistic abuse. Where activity like cyberstalking, sexual exploitation, and hate speech are often 'against' user licensing agreements on large online platforms, reporting capability and enforcement mechanisms for user bans are sorely lacking in nearly all cases. Platforms pay little heed to the unique experience of being a woman online, with policies failing to explicitly address issues such as misogynoir, transmisogyny, gendered and racialized disinformation, sexual harassment, and image-based abuse. No platform emerged from UltraViolet's grading system with anything higher than a C- (Reddit), with Facebook receiving a D-, and Instagram an F.

The algorithmic amplification of incendiary or abusive content in an environment where puritanical ideologies aim to suppress women's rights has thoroughly gendered implications. That the radical 'free-speech' ethos of social media has been dogged by the rise of extreme far-right hate groups that attack influential women attests to the need for further regulation in Silicon Valley. However, until this new regulatory environment dawns, it is important that women participating online are able to recognize the signs of gendered online abuse and disinformation so that, together, we might begin to mitigate its worst effects.

"Do not pretend it did not happen! Use your influence, power, and women's solidarity as a politician, to protect all women in your country and to force global platforms to eradicate efficiently misogyny and gender-based violence."

Sonja Lokar, Slovenia,
International Gender Expert



PREEMPTIVE ACTIONS

Preventative action to enhance your digital security

Strengthening Digital Security

Although it can never be foolproof, adopting comprehensive cybersecurity measures, building supportive digital communities, and tightening your digital hygiene before attacks occur are the best strategies for minimizing the harm of online attacks.

Most of the existing advice for women avoiding harassment online exists in this space, primarily agreeing on the following steps for prevention:

> **"Used well, social media has an amazing potential to enhance young women's voices and their engagement in a political career, but for women, coming across as inauthentic and scripted undermines trust. To use social media effectively is to focus on the social part of it, not just the media part."**
>
> **Celinda Lake, USA, Pollster**

CREATE STRONG, UNIQUE PASSWORDS

» A strong password is at least sixteen characters and should contain a mix of upper- and lowercase letters, symbols, and numbers.

» Use a unique password for every platform. If remembering all of these passwords seems impossible, download a password manager which stores and encrypts all of your platform passwords. Recommended password managers include **LastPass** and **Dashlane** which offer free versions and **1Password** which costs money but **allows journalists to create accounts for free**.

» Avoid using familiar names/places in your passwords and swapping out letters for correlative numbers/symbols (i.e. @ for a). Think of creating a 'passphrase' rather than a 'password,' including a sentence or an array of words.

» Try using an automated **password generator** (If you're saving your passwords in a password manager, you won't have to worry about remembering an array of obscure, generated passwords)

ENABLE MULTI-FACTOR AUTHENTICATION ON ALL OF YOUR ACCOUNTS

- Set up an app like **Authy** or **Google Authenticator** for a layer of security that requires confirmation on a second device before your account can be accessed. One of these apps is more secure than using two-factor authentication with just your mobile number, as it is harder to hack.
- The most secure form of two-factor authentication is a physical security key that you have to insert into your device to log on. Check out options **here**.

TURN ON AUTO-UPDATE ON YOUR DEVICES

Turn on auto-update on all of your devices and accounts, so that security measures stay up-to-date.

BEWARE OF SPAM OR PHISHING EMAILS
Be cautious when opening unexpected/ unsolicited emails or messages. Don't open unexpected links or attachments without verifying them with the sender on a separate platform

USE A VPN
VPN technology connects you to a server through an encrypted connection, making it more difficult for anyone to access your data. Research VPN options here.

AUDIT YOUR OWN SOCIAL MEDIA
Before entering the public eye or as soon as possible, audit your own social media accounts and delete anything you wouldn't want circulated widely

SET UP GOOGLE ALERTS
Set up Google Alerts for your personal information to know if it ever appears online, as well as for your name in order to track circulating coverage

CREATE MULTIPLE ACCOUNTS
Create multiple accounts where possible to separate your public profile and your personal life.

Platform Privacy Settings

Google
Facebook
Twitter
Instagram
LinkedIn

On whatever platforms that you can, you should organize separate public and private profiles. Your public account should be reserved for content you wish to communicate professionally – for your campaign, with your constituents, or in your role as a journalist. All personal information, or content that you would have shared with your friends and family before having a public platform, should be kept to a private account that is further protected and less accessible. This account should have the strongest privacy settings on a given platform, and ideally should not be immediately recognizable as you. Here are the various platform privacy settings, compiled by PEN America:

Establish multiple email addresses – Professional to list publicly, personal, and "spammy" to sign up for email lists, etc.

When possible, avoid allowing access to your accounts from third-party apps or services. When places ask you to "sign in via Google or Facebook," create a separate account instead.

Resources on Digital Security

C.O.A.C.H: Crash Override's Automated Cybersecurity Helper

COACH walks you through the individual steps of locking down your digital security and provides links in order to do so. It takes you through strengthening the security of your online accounts, hiding personal information, fortifying your websites, making it harder for people to take control of your computer or phone, and cleaning up/removing old accounts.

The Empowering Internet Safety Guide for Women

This guide, created by women and for women, focuses exclusively on digital security measures, breaking down the steps to take to protect yourself on specific social media platforms including Twitter, Facebook, Instagram, Snapchat, and LinkedIn.

PEN America Online Harassment Field Manual

The PEN America Online Harassment Field Manual offers resources and strategies for women, BIPOC, and LGBTQIA+ writers, journalists, artists, and activists who are disproportionately targeted by online harassment. It breaks suggestions down between those being targeted, witnesses/allies, and employers. Advice and resources are broken down into preparing for online abuse, responding to online abuse, practicing self-care, legal considerations, requesting and providing support, and defining online abuse. The manual is one of the more comprehensive out there in terms of walking through preparing for/preventing online abuse, handling attacks that occur, and what to do as a bystander.

Dealing with digital threats to democracy: a toolkit to help women in public life be safer online

This guide, compiled by **Glitch**, walks through digital security steps that you should personally take as a woman in the public eye, steps your team should be taking, ways to remain vigilant, and particular steps for staying safe on social media. The guide is comprehensive and should be studied and utilized both by candidates and women in leadership, as well as the teams that they have working around them. Glitch breaks their guide into three sections: Practice digital self-defense and self-care, Become an online active bystander to support those experiencing online abuse, and keep your supporters safe online.

Safe Sister Guide

The Safe Sister Guide walks through digital security steps to secure your online accounts, focused specifically on helping women and girls in Sub-Saharan Africa. It follows a character, Aisha, as she navigates digital security, offering readers the steps that they should be taking to protect their own information online.

The New York Times Social Media and Privacy Checklists

This guide walks through the basic, overall steps that you should take to protect your personal accounts, before breaking down checklists for specific steps necessary to protect your privacy online on the various social media platforms.

Heart Mob Safety Guides

In partnership with each of the following social media platforms (Facebook, Twitter, Reddit, Tumblr, and YouTube), these guides attempt to break down the privacy and reporting mechanisms that exist on each of these platforms and how to use them to best protect your digital privacy.

Fair Fight

5 Steps to Take if you EXPECT TO BE Targeted by the Far-Right
Fair Fight offers the following five top steps for precautions to take if you believe you're in a position to be targeted by the far-right when entering the public eye:

- Remove as much of your private contact info from the internet as possible
- Know which agencies/companies, if applicable, you can turn to for security
- Know what information about you and your family is already available via online search
- Always use secure communication, like Signal, and two-factor authentication
- If possible, lock down your personal social media and remove information about family members

Reducing Your Vulnerability to Doxxing

Doxxing is a type of online harassment that involves publicly revealing a target's personal information (i.e. address, contact info, job, family details, or other revealing information), often with malicious intent. Doxxing can lead to very real threats/harm, including stalking and harassment and physical violence.

In a 2017 **study** by Amnesty International, 17% of women who had experienced online abuse or harassment had had their personal information revealed. US activist and blogger Pamela Merritt talked about receiving an email from the FBI needing to talk to her about a white supremacist that was actively seeking out her home address in response to content posted on her blog. Colorado State Senator Rhonda Fields reported on this phenomenon to PBS NewsHour after her daughter's name and information became a central theme in attacks against her. Having previously lost a son to gun violence, she **commented**, "I just thought this came with the job, but when they used my daughter's name, when they said, 'We're going to come after you and your daughter and your family, and there will be lots of blood,' that's when it became real, I had already lost a son to gun violence, but now you're talking about going after my daughter, my only surviving child."

"Women in politics don't have to take the abuse online. There are ways to fight back, by implementing preventive measures, having a plan in case of doxxing, and to report the abuse. Taking these steps are a must for any woman in the public eye."

Vanessa Cardenas, USA,
Deputy Director at America's Voice

Steps that can be taken to attempt to protect your personal information online and attempt to avoid non-consensual release of any personal information are as follows:

01

Google yourself to see what identifying information is already out there. If there is anything that may be personally risky (private information such as address, contact information, etc. or anything you wouldn't want in the hands of the general public) try to get it taken down before your public presence increases.

For reference, gendered disinformation campaigns specifically build on, and are rooted in, deeply set misogynistic frameworks and gender biases that portray masculine characteristics as those fit for leadership while painting women leaders as inherently unfit through a selection of narratives rooted in classic misogynistic stereotypes.

02

Content to watch for. Note that these are the topic areas that may indicate you are part of a targeted attack: →

Untrustworthy - content that indicates women do not deserve the trust of voters or can't handle the basics of the job

Unqualified - attacks on qualifications can build over time and are rarely based on a woman's actual qualifications, and while voters assume men are qualified women have to prove it over and over again

Unintelligent - displaying women as dumb to send subtle or overt signals that women don't belong in politics

Unlikeable - likeability **has been shown** to be a stickier issue for women compared to men, with voters willing to vote for men they believe are qualified but do not like, but less likely to do the same for women.

Sexualized attacks - women leaders are often baselessly accused of being more sexual or libidinous than their male counterparts, or of using their 'sex appeal' to 'get ahead' in masculinized professional contexts. These attacks are often reinforced by image-based abuse, including non-consensual sharing of intimate images, the creation of deepfakes falsely showing women in compromising positions, or cherry-picking images of lookalike women engaging in allegedly 'unprofessional' behavior.

03

Invest in a privacy service such as PrivacyDuck or DeleteMe that can remove you from data broker sites, such as Whitepages, which allow people to buy your contact information. Go through the opt-out steps for individual servers **here**.

04

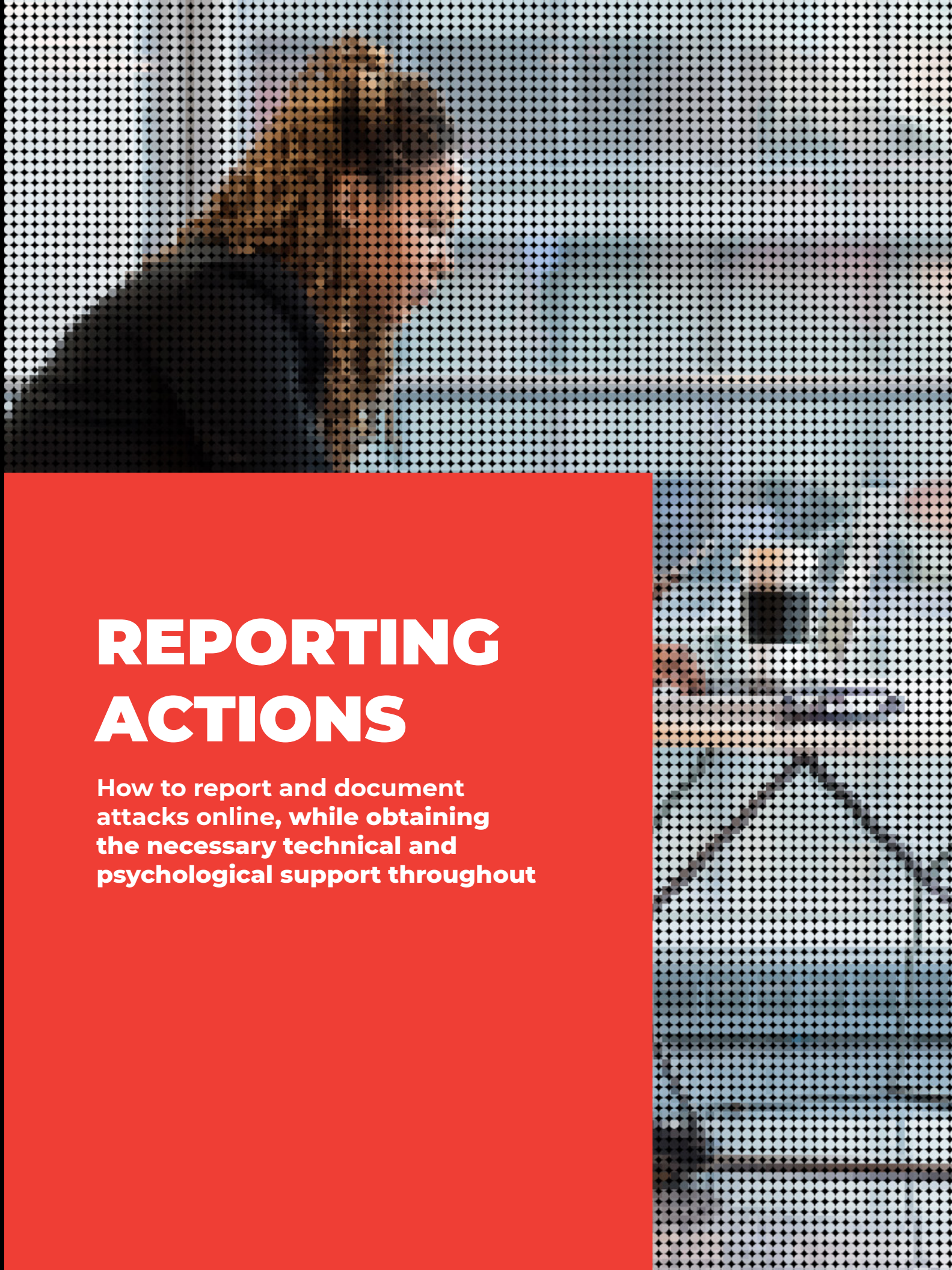
Avoid using geotag functions on social media that identify where you are when you post, unless you have already left the location. Review your location-tracking settings on your device and restrict location data on as many apps as possible.

05

Check on https://haveibeenpwned.com/ to make sure your email account and/or password have not been involved in any data breaches that could put your information at risk.

06

Make sure photos posted don't include identifying data, such as frequented locations. Consider scrubbing metadata from posted photos which can include the time, date, and location a photo was taken. To do so, you can run photos through a platform like **Image Optim**.



REPORTING ACTIONS

How to report and document attacks online, while obtaining the necessary technical and psychological support throughout

Reporting Digital Harassment and Documenting Abuse

When receiving hate online, deleting the messages may feel like the best way to handle the abuse you're seeing. However, even though it may feel counterintuitive, the best thing that you can do is document all the online abuse you receive. By keeping a record, you have evidence of the perpetrators, can observe patterns in abuse, and have evidence for if you decide to report the abuse to your employer, the platforms, law enforcement, etc. This process for reporting will also be walked through in the bullets below.

However, social media platforms are notorious for failing to act on reports they receive, failing to act on their own policies when they aren't being held accountable. As a recent **test**, the Center for Countering Digital Hate reported 300 tweets that contained misogynistic abuse. After 48 hours, 97% of them remained up on the platform. Further recent research shows that platforms that have received user reports have failed to act on 87.5% of Covid and vaccine misinformation, 84% of content featuring anti-Jewish hate, 94% of users sending racist abuse to sportspeople, and users who repeatedly send hateful abuse. Although Big-Tech cannot be trusted to self-regulate, documenting your abuse can still be useful:

> **"Try and build a mental wall between you and the vile online sexism. The authors will never treat you fairly so don't take their sniping to heart. You are a target simply because you are a woman."**
>
> **Julia Gillard, Australia,**
> **Former Prime Minister of Australia**

WHAT MESSAGES SHOULD YOU DOCUMENT?

Threatening or harassing emails
- When saving emails, make sure that you **include the original IP address** which could have identifying information about the sender

Screenshots and hyperlinks of social media posts/messages

Harassing texts and phone calls

If you cannot capture the full volume of online abuse, focus on attacks that are especially abusive or threatening, repeat offenders, and abusers using their real names

HOW SHOULD YOU LOG ONLINE HARASSMENT

Take a screenshot

- PEN America outlines here how to take a screenshot depending on the type of device you are using.
- Save all of these screenshots to a common file

Create a log of online harassment

- Make a document including the date and time of attacks, type of electronic communication, location/site where the attack occurred, nature of the attack (threat of sexual violence, racially motivated, etc.)
- See a sample log from the National Network to End Domestic Violence here and this checklist on obtaining proper documentation from Online SOS
- Consider having a trusted friend or co-worker help with/take the lead on the documentation process

IF YOU WANT TO REPORT YOUR ABUSE, HOW SHOULD YOU GO ABOUT IT?

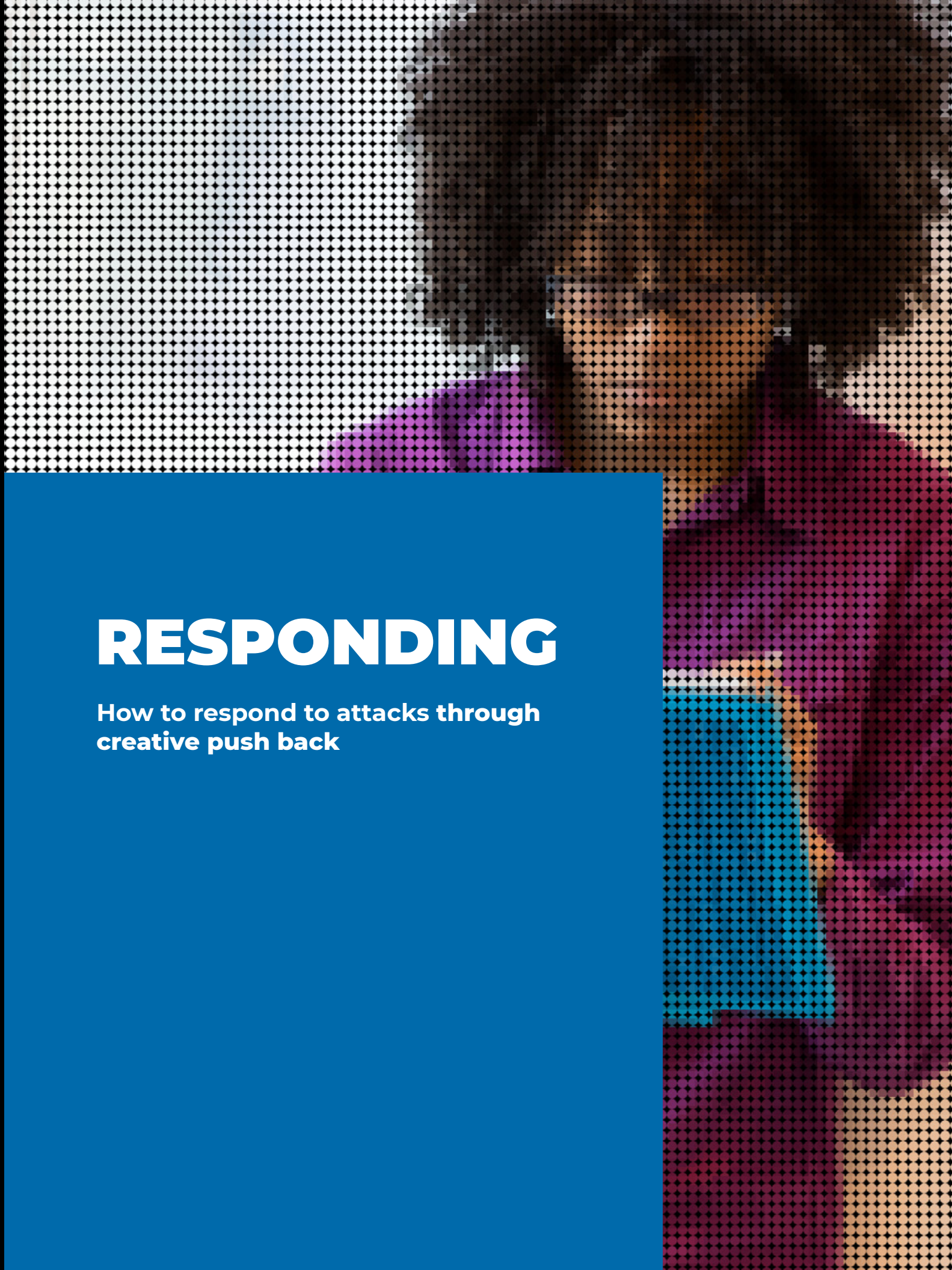
Reporting to platforms

- Take a look at this PEN America guide outlining how to utilize reporting mechanisms on various social media platforms

- Reporting keeps a record of abuse. It can be a helpful mechanism and sometimes will lead to the removal of content or abusers from the platform. However, studies show that platforms often fail to enforce their own regulatory measures, leaving up content that goes against their terms of service and allowing abusers to remain on their platforms. Facebook/Meta, for example, has policies against threats of violence, hate speech, violent and graphic content, nudity and sexual activity, cruel and insensitive content, manipulated media and deepfakes, fake accounts and coordinated inauthentic behavior, yet digital forensic analysis, and even unsophisticated searchers, demonstrate that gendered disinformation which violates such policies is thriving on social media platforms. This illustrates the larger need for platform reform and pushback on gendered disinformation beyond the level of individual online security.

Accountability Failure

Reporting mechanisms, whilst an important first port of call, rarely translate into direct action or account bans, as platforms have a history of ignoring them. In 2022, the Center for Countering Digital Hate (CCDH) conducted a study on the Instagram accounts of five high-profile women. It found that reporting hateful or violent messages resulted in the abusive account being removed in only one out of every ten cases, despite the account violating the platform's content policy in each instance. According to CEO Imran Ahmed, "misogynistic abuse and threats sent by abusers with impunity" is the "cost of admission" for public-facing women on social media.



RESPONDING

How to respond to attacks through creative push back

Fighting Back: Responding to Online Abuse & Changing the Discourse on Women and Leadership

Different incidents of harassment call for varied responses. Sometimes, responding to harassment can be dangerous, spreading attacks and disinformation and expanding the platform of your online abusers. Sometimes it's not safe to respond to your abuser and could risk exposing personal information.

However, other times, in pervasive attacks, a response can be warranted and can allow you the ability to expose abuse and push back on the perpetrators, platforms, and general misogynistic narratives. On a widespread scale, #ShePersisted **helped to organize** a **letter**, co-authored by U.S. Representative Jackie Speier and signed by over 100 current and former women legislators globally, that **asked Facebook** executives to stop the spread of gendered disinformation and online attacks against women on their platform.

Whilst this was a group effort, sometimes it can also be effective and empowering to respond on a personal level. This, when done carefully and in a considered manner, can offer a powerful opportunity to reshape the narrative surrounding your character and leadership.

"You can blow out a candle or douse a flame but you need a team to put out a blaze. Call for help sooner rather than later."

Rumbidzai Chisenga, USA, Director of Programs at the Ellen Johnson Sirleaf Presidential Center for Women and Development (EJS Center)

Examples of effective push back

A prime example of this sort of pushback comes from First Lady of Namibia Monica Geingos, shown in this video. She wrote, "When there was a clear social media campaign of anonymous WhatsApp messages specifically targeting me in the most disgusting ways, and I was told not to respond but to ignore and I did. But it was a mistake, your silence will not protect you." Specifically, she argued that women allowing and ignoring violence and bullying online can signal that conduct like that is normal and acceptable online. As bystanders or targets, she recommended challenging gendered violence by standing up for women online.

In the lead up to Kenya's 2017 general election, with support from USAID, the International Foundation for Electoral Systems launched the #BetterThanThis Campaign, an emotive and dynamic digital campaign which sought to address the sexist barriers faced by women in Kenyan politics. Instead of simply focusing on the abuse messages, however, the campaign engaged viewers with an aspirational message at its core, appealing to Kenya's sense of national pride and desire to be "better" than the sexism shown to its women leaders. In a video called "**Ugly Words**" that went viral and spared substantive engagement online, the campaign centered on exposing violent rhetoric documented toward women in politics as evidence of the sexism and misogyny that undermines women's leadership and electoral outcomes. Through a dynamic social media strategy, the campaign showcased what Kenya is missing without adequate political participation of women vis-a-vis women's leadership across all the socio-economic sectors of the country.

Former Canadian Minister of Environment and Climate Catherine McKenna exemplified this advice when she pushed back in response to a Conservative MP referring to her as "Climate Barbie:"

Kyiv Post

Olga Rudenko: Stop beauty-shaming women

By Olga Rudenko. Published Jan. 20, 2015. Updated Nov. 6 at 11:14 am

When there is more exposure and visible pushback around gendered disinformation examples in real time, male allies can more easily step in to do their part to signal that it doesn't have to be this way.

Women in leadership in Ukraine are commonly the subject of misogyny and abuse for their appearance and perceived sex appeal. In 2015, the deputy Minister of Interior in Ukraine Eka Zguladze was attacked on Facebook during a press conference on police reform. She was subject to an online attack with a faked image of what appeared as a drunken pantyless double, an attempt to disgrace her and distract from her message as a public servant. This was despite the woman photographed not actually being Zguladze, with no context behind the picture, which is another form of image-based abuse of women.

The origins of the attack were not clear, although a common tactic of **Russian-oriented disinformation** campaigns is to undermine women leaders with faked images and dehumanizing content. A reporter covering the press conference took matters into his own hands, writing an editorial speaking out about this abuse, telling his compatriots to quit "beauty-shaming" women. "This is a very sorrowful trend because of what it indicates – a vulgar, rudimentary society. Beauty is irrelevant to a woman's career. Red lipstick can be worn by a top professional. Sometimes a short skirt is just a short skirt. There are no intellect markers in a person's looks – they are in the person's work."

"I was able to change negative perceptions about me, using social media to promote my projects, and often receive messages from people I don't know personally congratulating me for my work."

Comfort Doyoe Cudjoe-Ghanash, Member of Parliament, Ghana

Below, find best practices for responding to online hate, and when to do so:

How to decide whether or not to respond:

01

Do NOT amplify a false claim

Engagement is currency - when you like, share, or respond to disinformation, it will be shared to a larger audience due to platform algorithmic preferences.

02

Assess the threat level for your physical and digital security.

For more detailed instructions on assessing threat levels, check out PEN America's guide **here**.
Key tips are below.

- Do not engage with legitimate threats to your own safety.
- Document and report your harassment.
- If your harasser is likely to continue harassing you online or escalate their harassment upon receiving a response, even if they pose no threat to your physical safety, it is likely not worth it to engage.

03

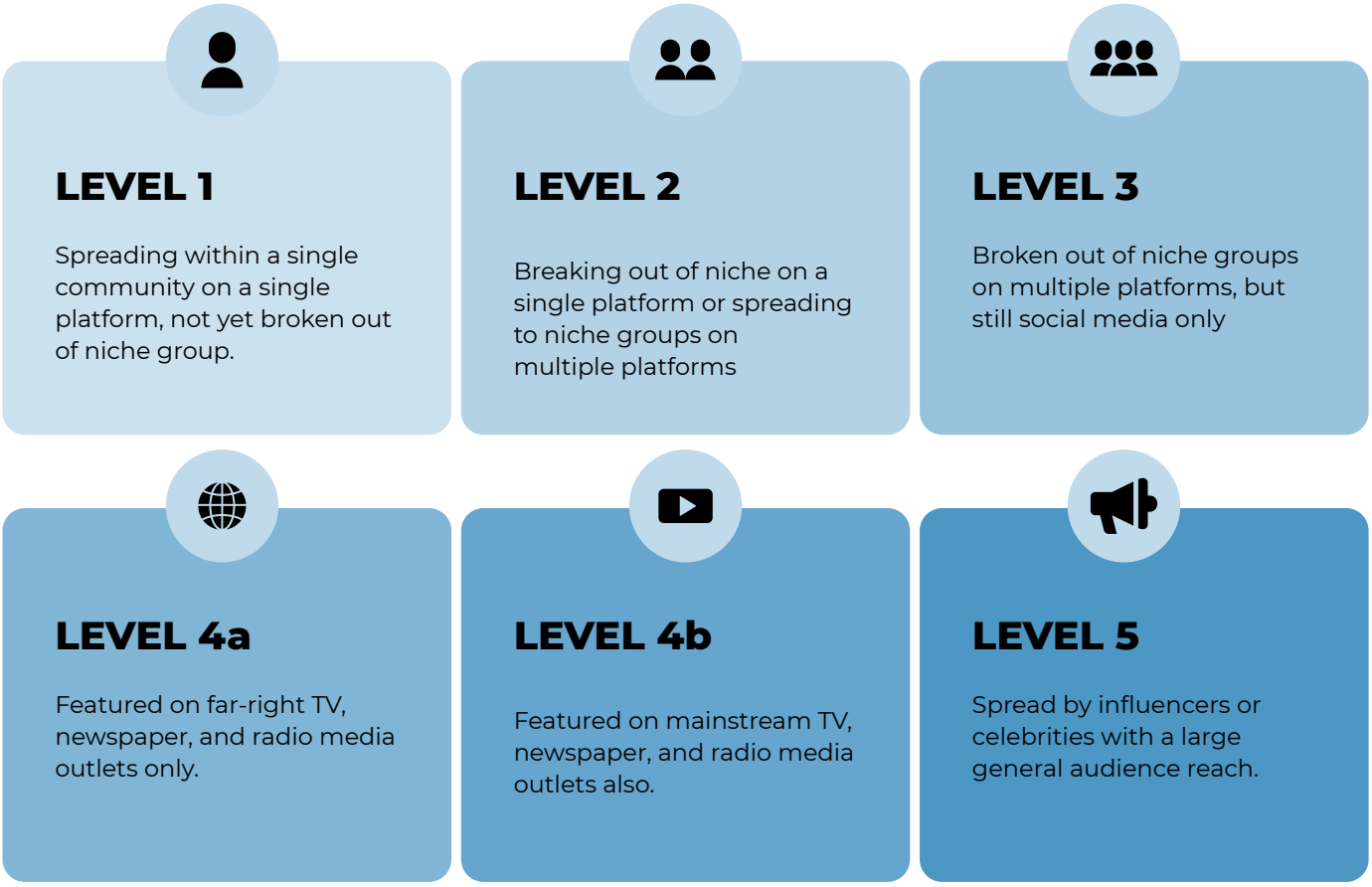
Evaluate the reach and impact of the attack.

- Reach: Are people seeing it already?
- Impact: Will it change the OFFLINE situation: votes, reputation, support?
- Our first goal is to do no harm, so if something is not getting real reach and impact, talking about it will make it worse.
- In considering reach and impact, also think **about:**

  - **Time horizon** - will this have a long term or immediate impact?
  - **Who are the actors?**
  - **What types of accounts are promoting the narrative?** Bots, fake news, trolls, deepfakes, etc.
  - **What types of disinfo are being promoted?** True, false, out of context, character attacks, etc.
  - **Have the attackers violated platform terms?**
  - **Has the attackers' impact been effective or just attempted?**

GQR

The following chart draws from Ben Nimmo's original **Breakout Scale** classification system, and its adaptation by the **Dewey Square Group**.



Evaluate whether you yourself are emotionally prepared for confrontation. PEN America proposes asking yourself the following questions:

- Are you constantly ruminating on the harassment? Do thoughts of your online harassment crop up throughout the day, interfering with your work or interrupting your social life?
- Are you more interested in retaliating against and humiliating your troll than in standing up for yourself and your ideas?
- When you think about your online harassment, do you get agitated and/or upset? If so, are you able to calm yourself down?

When a response isn't the proper option, don't be afraid to block, mute, and restrict abusers.

Blocking – Blocking a user on a social media platform restricts their access to your account and the content you share and makes their content invisible to you. Although users will not get alerted if you block them, they will be able to tell if they visit your profile which can exacerbate matters in certain circumstances.

- Try out the **MegaBlock** extension - "Don't like a bad tweet? Block the tweet, its author, and every single person who liked it—in one click."

Muting – By muting content, you can hide certain content from only yourself so that it's not visible to you by default. Depending on the platform, you have the option to block accounts, comments, DMs, and specific content.

Restricting varies from platform to platform. Check out the **PEN America guide** here on how to utilize blocking, muting, and restricting on each platform.

Currently, under US law, the ability for a person acting in a public capacity online (e.g. politicians using an 'official' account) to block other accounts is protected by the First Amendment. However, the propriety of this in terms of the Freedom of Information Act is **debated**, and political full-disclosure norms and rules are country specific. Generally though, public figures using social media in a personal capacity are free to block whomever they please under all platforms' terms and conditions, regardless of whether they occasionally use their account in an official capacity. The decision to block should be weighed seriously, as the reaction of blocking someone may gain more attention than the abuse that generated the necessity to block.

Having a network of supporters can be essential for the purposes of response as well. Pollster Celinda Lake considers that the most effective way for a politician to diminish its impact is to build a community of supporters who will pile onto the aggressors when they post harassing comments on social media. "As more women politicians use social media to build connections with more people, the potential to drown out the misogyny and harassment grows."

"We must be strong, convinced of our choices and committed to our political battles! Always denounce haters"

Valeria Fedeli, Italy, Politician and former Minister of Education for Italy

"For far too long women public leaders have been traumatized and silenced by online attacks. No more. Now is the moment for the world to be aware of how debilitating this online behavior can be and for women leaders to stand up to faceless bullying and fight the increasing threat of disinformation and safeguard their leadership which the world needs most desperately now."

Manira Alva, USA, Vice-President of Issue Advocacy at Vital Voices

The best digital infrastructures are self-sustaining and facilitate organic engagement from a network of people who operate as a community. Building relationships with supporters can help create an army of allies and inoculators to share proactive messaging on your behalf. Content shared by this community of allies will have a built-in layer of trust within their networks online.

If you want to respond, how should you do so?

The Barbara Lee Family Foundation **explains** still that silence isn't always the best option. When misogyny is used to attack women leaders online, ignoring or being perceived as turning a blind eye to serious incidents of sexism can potentially result in blowback against women candidates because voters want to see strength and backbone. In some cases, voters view a woman candidate's responses to sexism as a demonstration of her leadership and electability – not something that weakens the perception of her electability.

When addressing an attack that is specifically sexist

- **Be authentic** - Use a personal narrative, which can connect to voters on universal values (i.e. equality, fairness, what is best for all women and girls)
- **Utilize validators** from your network of support to affirm your pushback and counter-narratives
- **Emphasize** the severity of the issue and contextualize why it is harmful
- **Keep in mind** that a woman's race and age can unfortunately impact how pushback is perceived.

Sample language:

- "This has no place in the media"
- "My appearance is not news"
- "Don't depict women as being less serious and having less to offer"
- "Much to offer my constituents"
- "Damages our political debate and democracy"

In responding, focus on what you can control

Use your trusted voice within your own network

Share positive information

Amplify the content you want to spread

Target your message when you can

tag friends, send DMs, use the platforms where your networks are.

Often a response does not need to entail naming or directly addressing your abuser. In the instance that attacks are coming from more than one person, it can be impossible to do so. Additionally, by not replying to or directly addressing your attackers, you're able to address your concerns without spreading their attacks or offering them a larger platform. Instead, consider:

Publishing a statement on social media condemning the type of harassment you faced and correcting the record if necessary,

Deploying your own online community to correct the narrative and share positive content,

Screenshot and share the abuse you've faced to call out the behavior.

- Be careful here about offering a platform to the attacks. Calling out the harasser directly could result in further abuse and should only be done if the attacks have already reached a widespread audience.

Use language that avoids escalating the attack as much as possible

Address the content of the harassment instead of personally attacking your harasser

Talk about the impact the harassment has had on you and the consequences of the online violence that you've seen

Emphasize your humanity, especially if there's a specific piece of your identity that has been attacked.

Counterspeech can also be a helpful tool for witnesses and bystanders. According to a study from the Economist Intelligence Unit and Jigsaw, **85 percent** of women globally reported witnessing online violence against other women. A coordinated response to attacks can be key to correcting the narrative and maintaining control. As mentioned above, having a network of people to help handle online abuse is essential, and this is another example.

"The more we normalize women in places of power and fight back collectively against this type of harm, the less we will see it. Continue to move forward, lean into your network of support and persevere. By running as our authentic selves we are opening up spaces for others - especially those from marginalized communities - to run as well. You are not alone."

A'shanti F. Gholar, USA, President of Emerge

Practicing Self-Care and Obtaining Psychological Support

Online harassment and attacks can feel isolating and often out of your control. On a panel featuring Canadian women leaders, former journalist and parliament candidate Tamara Taggart **explained** how, during her run for office, she became the target of intense gaslighting and trolling online, including references to her disabled son. Due to the treatment she received online, Taggart has concluded that leadership is not worth it — "I would never ever, ever subject myself to that again. It has damaged my mental health. It has made me fear for the safety of my family. It has made me fear for my safety." All the women on this panel emphasized feeling a deep sense of loneliness in the face of abuse online, and reported being uncertain of existing resources for support or steps that they could take.

It is essential that you take care of yourself and have people who can support you through any harassment that you may receive. Below are steps to protect your own wellbeing, as well as existing resources for psychological support for women leaders:

Tips from Pros

- **Avoid looking at harassment.** Consider having a trusted friend or team member review content in your mentions for you and ensure personal information is not being shared.
- **Seek expert support** - Take a look at the resources at the back of this guide for the types of resources you may need.
- **Take advantage of blocking or muting abusers** and/or use the "hide replies" features on platforms like Twitter to limit the abuse you are seeing. A lot of advice in the US-context advocates using these features generously, and not being afraid to employ them. Before taking these steps, however, ensure that there are no laws regarding blocking individuals in your country.
- Remember, **you are NOT to blame for online harassment**.
- **Create support groups** that can exchange strategies for dealing with harassment and provide emotional/practical support.
- **Create online boundaries** and establish them with your team. Have a page or a pinned post that explains the type of content that you will or will not engage with.
- **Spend time offline**. Take breaks and have someone on your team take a turn managing social media accounts when you need to be off of them. Set the expectation with your team that time off of social media is acceptable.

During a major attack:

Tell your team/network what's going on so that they can support you.

Take a look at PEN America's **guide to talking to friends and allies about online abuse**

Log off and lock down accounts for at least 48 hours.

Document the attacks. (More on how to best do this later in the guide)

Further Resources for Self-Care and Psychological Support:

If you're experiencing anxiety or depression symptoms that don't go away or are interfering with your professional or personal life, you may want to consider speaking with a professional therapist or counselor. Find online therapy and mental health-oriented apps below alongside resources that help with providing therapy or funding for psychological support for journalists:

IWMF United States Journalist Emergency Fund

Funds that will support journalists with trauma, mental health services, legal aid, etc. who demonstrate financial need.

The Black Journalists Therapy Relief Fund

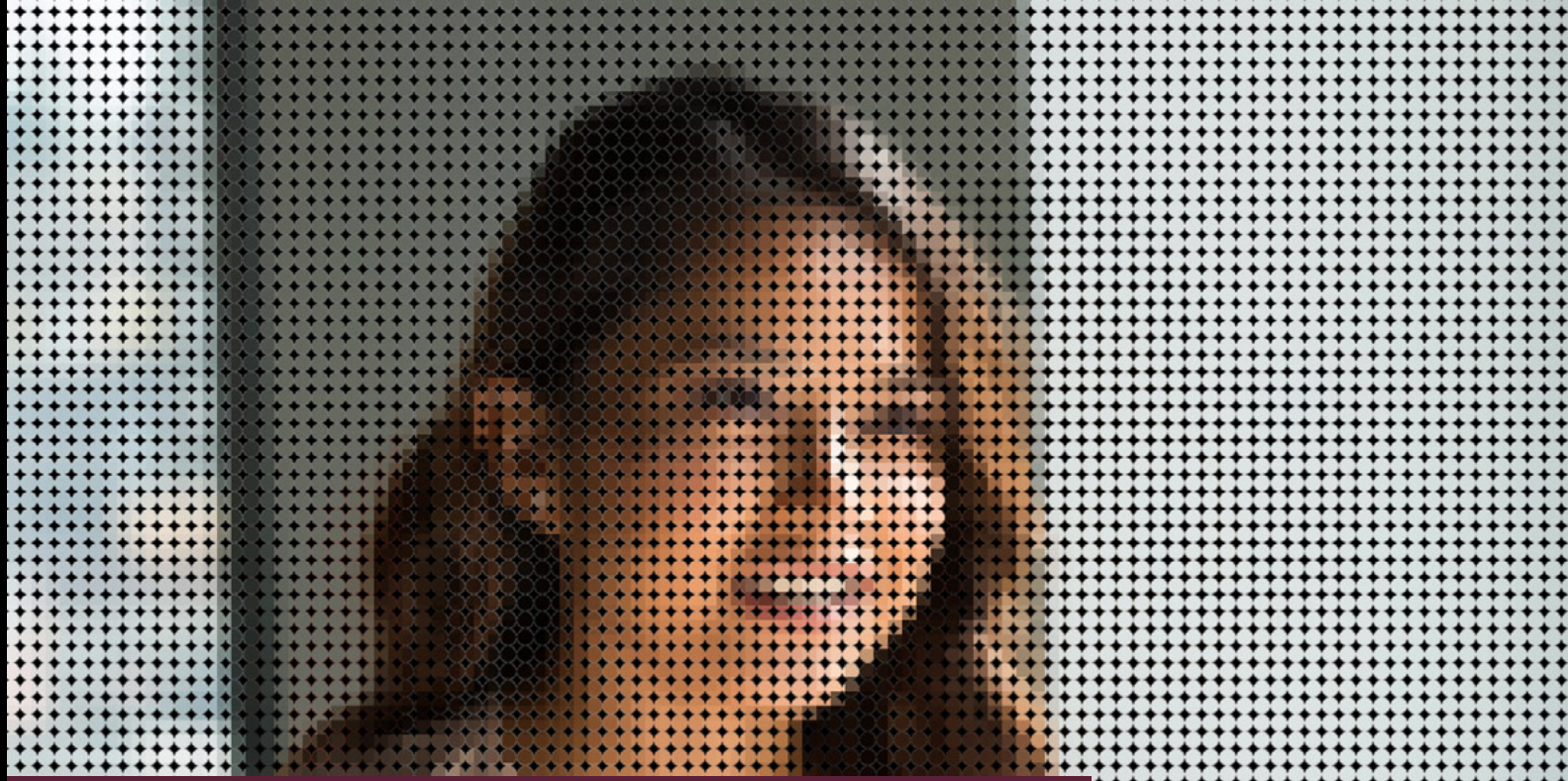
Funds that support Black journalists who are struggling financially to receive mental health support

IWMF Emergency Fund

Provides women journalists funds supporting, among other things, small grants for psychological and medical care for incidents directly related to threats and crises caused by one's work as a journalist; Three months of temporary relocation assistance in the event of crisis or threat; Non-financial assistance in the form of information about additional access to resources.

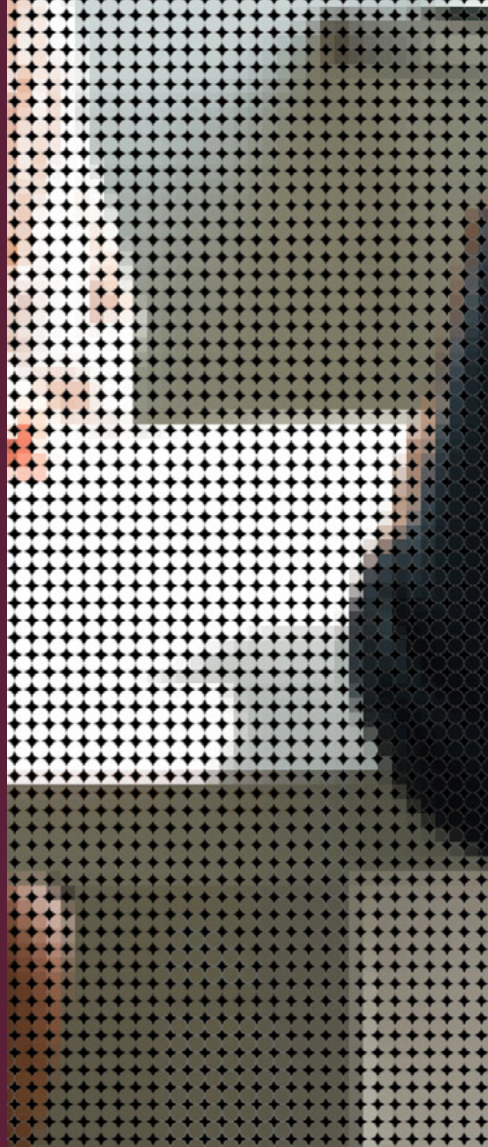
The Rory Peck Trust General Assistance Fund

The Assistance Grants are meant to help professional freelance journalists (and/or their family) who are facing a crisis directly related to their work.



REPRODUCTIVE RIGHTS

Speaking in support of sexual and reproductive health when under ideological attack



The Abortion Rights Debate:

Speaking in Support of Sexual and Reproductive Health When Under Ideological Attack

This section was a late addition to our Digital Resilience Toolkit, brought about by the monumental shift in the women's sexual and reproductive health (SRH) landscape in May 2022, when a draft US Supreme Court opinion that supports the abolishment of Roe v Wade was leaked. More and more liberal democracies seem to be gearing up for a prolonged battle centrally concerned with women's rights and abortion, with the US closely following Poland and Hungary in a move towards implementing anti-democratic, patriarchal policies that remove access to safe and legal abortion care. After the leaked opinion, it became clear that much of the public discourse women leaders can be expected to face and contribute to in the coming months and years will involve abortion and SRH issue-sets, and so it was vital to include online messaging strategies about these contentious hot-button issues.

Since 2018, #ShePersisted has conducted first-person interviews with dozens of activists, journalists and women in politics across the world about their experience with gendered disinformation. Nearly all of them reported receiving threatening, horrifying attacks on social media platforms.

"The first time I had an opinion piece published at the national level, my colleagues warned me to take care of myself. They said: 'don't read the comments.' And of course, I read anyway. Preparing women for leadership should never entail preparing them for hatred and online violence, but this is part of our reality. I take comfort in knowing that owning your power means knowing how to take care of yourself and your safety first then using this power to shape policy, advocate and promote accountability and justice. This is how we make change"

Sara Guillermo, USA,
CEO of Ignite National

Some of the most vicious and coordinated online attacks reportedly occur when women speak out to protect and advance women's/human rights, migration/immigration debates or on climate change issues. Women's sexual and reproductive rights – particularly abortion, as well as LGBTQIA+ rights – are among the issues that women in public life report getting viciously trolled and threatened around most.

Trend Analysis: Targeting of Women Leaders Speaking for Women's Rights

Democratic backsliding

The reality is that women are on the frontlines of the fight to protect essential rights and liberal values. Their powerful voices represent a threat to authoritarians and illiberal actors everywhere. Silencing them is the most effective way to undermine those rights and erode democratic institutions. Rolling back abortion rights is rare in democracies, and is a sign of democratic backsliding. *Keep track of the latest developments by referring to the Center for Reproductive Rights* **global map** *of policy proposals.*

The global threat

According to the **Observatory on the Universality of Rights**, anti-gender actors using arguments based on anti-rights interpretations of religion, culture, and traditional values have made significant strides recently in implementing and institutionalizing a regressive agenda within their Parliaments and in international bodies such as the UN. Many far-right actors have creatively and effectively dominated the battle for rights in language and rhetoric with increasing success, towards their goal of undermining gender and sexuality-based rights.

Role of social media

Social media has been providing authoritarians and some of the most destructive forces in our societies with new and exceptionally powerful tools to undermine human rights and democracy, increasing hate and destroying social cohesion. Divide and conquer isn't a new strategy, but because of social media it is now being applied at a speed and global scope that are unprecedented, and without any accountability for the digital platforms that are enabling it.

Targeting aims

The opposition to sexual and reproductive choice hinges on targeting women, girls, and LGBTI people. Attempts by anti-democratic actors to create fractures along the lines of gender identity and expression are very intentional, and often taken to scale through online attacks by proponents of anti-gender ideology.

Digital platform reform

We cannot simply continue sacrificing decades of social and political progress on the altar of Big Tech's greed and incompetence – we need better digital platform standards now and governments to take a duty of care position over their populous.

Message advice for women in politics

Key Takeaway: Prepare a Winning Message Formula

Every online interaction is bespoke, and therefore context is crucial for engaging properly with issues this fundamental. However, there are ways of structuring your messaging strategy to represent yourself and your views in the best possible light, and present a persuasive pro-compassion feminist position.

Refer to **research** conducted by Anat Shenker-Osorio and the Center for Community Change (CCC), for direction, and in a related **Messaging Guide.**

01

MORALIZE THE ISSUE POWERFULLY AND IMMEDIATELY.

Framing conversations about abortion through a values lens, rather than a problem-focused strategy, is a winning approach. When the two broad opposing viewpoints on abortion are properly analyzed, it is clear that the pro-choice (or pro-compassion) stance is far more 'pro-life' or 'pro-family' than the pro-forced pregnancy camp, as women's flourishing is placed at the center of an ethical discourse.

02

MAKE CLEAR WHAT IT IS YOU'RE UP AGAINST.

While it's not helpful to highlight problems only, it's still important to convey what's at stake. Oftentimes, giving a face to the issue (explaining who is behind these structural inequalities) can be helpful. Wherever possible, describe what movements or individuals are behind the problems identified, e.g. 'lawmakers are putting up barriers to prosperity'.

03

SUBSCRIBE MOTIVATIONS TO THE OPPOSITION.

Ask why are opponents really fighting this political battle, what is their ultimate goal, and how far might this continue to go? Speak to your opponent's motivations and how these conflict with shared values held by the majority of reasonable people in your democracy (for example, statistics show that the majority of citizens in liberal democracies hold pro-choice values).

04

OUTCOME OVER PROCESS.

When communicating about a policy change it's important to not focus on the material process of the policy proposal itself, but on what the policy aims to bring about - the outcome. It is then easier to create a more persuasive, values-based conversation when it is future-oriented.

05

EXPAND YOUR MESSENGERS.

Enlarge the constituency you are working with. In some countries, religious groups can be strong and effective allies that challenge a myopic position against abortion presented by the opposition to the public. Faith-based leaders can provide valuable talking points as well as be spokespeople. Nurses associations and health care professionals are a natural ally in many places.

Going Deeper: Features of a Winning Message Formula for Women's Rights

Lead with values

Pro-human rights messengers tend to come at political issues from a problem-first lens. As the CCC **points out,** campaigns that fought for marriage equality in the 20th century became successful when they stopped talking about rights and started talking about values - in this case, the freedom to love. Facts do not change peoples' mindsets: values-based framing does. A values-based message allows more connection with people in order to find common ground and build consensus. Like-minded people can disagree on the details of a new initiative or proposed legislation and how to achieve it, but those same people can find common ground when it is framed in principles like opportunity, equality, family, and fairness. Connecting to an audience through words, images, symbols, and stories grounded in values helps make new avenues accessible in a way that touches on the emotional implications for individuals, their families, or things they hold dear.

Neutralize "wedge" issues by embracing them

Shying away from controversial issues, such as transgender rights, abortion, and sex work, is unproductive and plays into the opposition's hands. The best way to neutralize these attacks rests in addressing these issues head-on within movement conversations to create stronger, more explicit links. When sexism on the campaign trail in the United States was **researched** by the Barbara Lee Family Foundation, a majority of voters reported believing that women face sexism while campaigning, and they indicated broad support for women candidates speaking out about the sexist situations they experience. Voters expressed a clear preference for a calm, confident, and professional response—vs. angry or retaliatory—from a woman candidate in response to sexism. Ignoring or being perceived as turning a blind eye to serious incidents of sexism, or controversial issues around women, can potentially result in blowback against women candidates because voters want to see strength and backbone.

Don't amplify your opponent's message, or think fact-checking is good enough

Much of the anti-abortion rhetoric is some form of mis- or disinformation, or based on a series of false binaries. Do NOT amplify this kind of mis- and disinformation. Which means, don't retweet/repost it even to refute it; doing so will only boost the algorithms, which means more people will see it. Repeating a false claim—even to debunk it—makes people more likely to believe the claim is true. Fact-checking false claims has been **proven** to improve the accuracy of audiences' factual knowledge, but it has far less impact on their beliefs and actions, particularly when gender is at stake. Therefore, merely correcting the misinformation doesn't remove the emotional attachments certain audiences have with the sentiment of the lie being spread, and risks amplifying the mis- or disinformation fueling false beliefs.

De-escalation Strategies

Given the empirical evidence that the most vicious and coordinated online attacks reportedly occur when women speak out to protect and advance women's rights, it is necessary to prepare for a contentious period that can potentially escalate into violence as abortion rights continue to be attacked around the globe.

Know the landscape:
Anti-rights actors and extremism

In the United States, the draft opinion of the Supreme Court that supports the abolishment of Roe v Wade is a startling setback for intersectional equality and women's rights. It is not, however, unprecedented in light of a global campaign to undermine women's reproductive choices, and can be seen as the culmination of efforts of the extreme right to mainstream damaging misinformation and virulently anti-equality messaging from the political fringe for many years now.

Far-right extremist groups have a history of scapegoating abortion as a wedge issue with which to shoehorn radical ideology into accepted discourse. These groups have long honed their rhetorical tactics online. Many liberal democracies such as the US are now at a crucial turning point (one that many countries such as **Ireland** have found themselves at in recent history) where the scale could tip for or against democracy and compassion. It is important to get our messaging right while at this crossroads.

As the recent spate of far-right terror attacks by individuals citing gendered ideology attests, anti-genderism, anti-abortion, and far-right extremism are an interlinked phenomenon. They are thought positions inherently linked to violence. Terrorist attackers in Christchurch, New Zealand in 2018, and, Buffalo, New York in 2022, namechecked the '**Great Replacement**' conspiracy theory as an impetus for their horrific, murderous acts. This racist, blatantly false conspiracy narrative has been spread by right-wing TV commentators like Fox TV's **Tucker Carlson**, alleging that white people are becoming a minority in the West due to high rates of immigration, and low birth rates. The anxiety shown in the Supreme Court's draft leaked opinion about the "supply of babies"

As the recent spate of far-right terror attacks by individuals citing gendered ideology attests, anti-genderism, anti-abortion, and far-right extremism are an interlinked phenomenon.

eerily echoes the great replacement theory, highlighting how these once peripheral racist and sexist ideologies are **manifesting**.

Conspiracy theories such as this one are a common thread that links anti-abortion movements to violent extremist actors. Abortion is seen by the far-right as an 'easy win' moralizing point through which to normalize further extremist thought, including extreme racism. As well as these recent examples, the anti-choice movement itself has a long history of violence and terrorism in the United States especially. According to **NARAL Pro-Choice America**, from 1977 to 2020, anti-abortion violence in the US has led to 42 bombings of health clinics, 194 incidents of attempted arson at clinics, 11 murders (including doctors and pregnant women), and 26 attempted murders.

Messaging in times of violence

According to **Over Zero**, in an atmosphere of heightened national tensions and rampant misinformation on social media, communication from local leaders and other credible and influential leaders is paramount in preventing, de-escalating, and even healing from intimidation, division, confusion, and violence.

01

Continue to promote positive norms and vision. Be FOR something not just against something. Tell the story of what IS rather than what is NOT.

For example: talk about all the people who worked together to ensure women's access to health care, and speak to how you will work across your community during this transition period. In Ireland, where abortion was legalized in 2018 after centuries of church incursion on state, many have attributed the success of long-fought women's rights campaigns to women from all areas of society coming together to speak about their own experiences of abortion. This not only helped normalize and humanize abortion as a procedure, but created a classless groundswell towards a common goal: safe access to vital medical care for women from all walks of life.

02

Show positive action as the norm - in messaging, and through examples and actions.

Whilst abortion is often coded as a "two-sided" issue, in reality, polling from most liberal democracies has shown overwhelmingly that support for reproductive freedom is the norm, as seen from **this report** by NARAL on the U.S. landscape. The public is largely in agreement as to what's best for our families and communities, and that fact is often not widely known!

→ **For example:** While examples related to sexual and reproductive health are great, feel free to use other examples of positive, community-minded behavior as well. This can illustrate how far-reaching norms of care and cooperation are. For example: "In Durham we take care of each other, as evidenced by the incredible interfaith drive for hunger relief that resulted in 20,000 pounds of food being delivered."

03

When it becomes necessary to talk about negative behaviors and actions, or you want to make a statement condemning certain actions, remember that repeating a narrative can make it appear more prevalent/powerful, and focusing on someone's actions can serve to bring attention to them.

This can embolden bad actors to act out in order to provoke a reaction and engender discourse (the 'all press is good press' strategy), and make people who disagree with negative behaviors more nervous in speaking out about them.

04

When calling out negative behaviors, use a "norm sandwich": tell the positive first, then show that the negative behaviors are harmful and aren't approved of/engaged in by most people, and end on a positive, plus a call to action.

→ **Remember:** Where you see attempts to escalate a situation, sow tension and division, and shift the narrative in that direction, it can be tempting to respond and buy into those frames. If you buy into those frames and give them oxygen, you can inadvertently help build a story of division or fuel a narrative you're hoping to counter. Stay focused on what you are for and the types of actions you want to move people towards. Work to build momentum in that direction.

05

When you're rowing in a good direction, keep paddling!

If things are calm and good, don't rock the boat, move to positive stories about your community and keep channeling peoples' energies and actions towards those stories!

→ **For example:** Messages like "hate is everywhere" or "people are more divided than ever before" can exacerbate these dynamics; instead, consider "people are saying they are tired of division, and doing [xyz] about it."

Online approaches

It is essential to use your communication platform in concert with a broad set of influential voices to assert your commitment to democracy, safety and security of all people, accountability for extremism, and any attacks against women speaking about abortion rights. Communicate early and often, and use your platform to amplify voices of influential leaders in your community.

If you are attacked online for your position on reproductive rights, map out who your on-and-offline messengers are who can help stop the spread of a false narrative, and show support to your story. Who are the friendly media outlets and reporters you'll contact to tell your story? Who on your team will reach out to Facebook, Twitter and Google to advocate for a content takedown request? Be prepared. Think through the worst-case scenario in advance of it happening.

Offline approaches

If there is a violent outburst while campaigning or in office, be sure to connect and coordinate with key stakeholders. Often anti-abortion events, particularly during an election period, are planned with the intent of undermining democracy; of replacing debate, deliberation, and voting with violence and intimidation. It is essential to connect and coordinate with key stakeholders - internally and externally, from the local to the federal level - to ensure a consistent and well-coordinated response that leverages the full power of civil society (including organizers, business leaders, faith leaders, etc.) and democratic government.

Countering misinformation and using measured language in times of violence

Though it is rare, especially if all necessary safety precautions around campaigning on contentious issues like abortion care are taken, physical attacks against pro-compassion, pro-choice messengers can and have happened. As already outlined, anti-abortion lobbies and far-right extremists exist on the same violent spectrum, and hang out in the same clubs, where aggression is always the first response.

If you do witness or are involved in an offline attack, it's important to keep in mind a few procedural steps recommended by **Over Zero** that can help you get the appropriate response and, if needed, physical and psychological care.

01

Keep providing accurate information about what's going on. Provide correct information about the attack to official and trusted sources that will widely disseminate it to make misinformation less salient.

02

Be as specific as possible when referring to contentious claims or events. The more specifics that are provided, the less room there is for speculation.

03

Continue to avoid speculation and alarmism in your public communications.

04

Be cognizant of word choices and metaphors. Even if not intended to do so, language that compares events to natural disasters (e.g. "violence erupted") or compares people to pests, disease, etc. (e.g. "a swarm of people") can increase tensions and the risk of violence.

05

Remember: Never repeat baseless claims. This gives them more air. If you feel like you have to mention a claim, first tell the correct information. Use the **Dos and Don'ts for correcting misinformation.**

06

If you are considering talking about violence, use the **Dos and Don'ts for talking about violence**: provide context, show condemnation and positive norms, and be careful how you talk about groups.

Activating shared identities and values

01

Continue to activate and speak through pluralistic and cross-cutting identities. During periods of violence, it is critical to undermine a zero-sum narrative.

02

Tell stories of people engaging in positive actions now, and tie shared identities and values TO those actions.

03

Keep connecting to your existing network - see how people are doing, what they're thinking. Get on the same page and message one another. See how you can coordinate in your community based on what you're witnessing and experiencing.

04

Express gratitude to people who are modeling positive behavior. Again, tie this behavior to values and shared identities when possible. This can be through your public messaging, but also through reaching out directly to local officials in your community who you see standing up for democratic processes - let them know you appreciate it!

RECOMMENDED RESOURCES

Many organizations have sought to provide advice on digital security, online safety, and lessening online abuse and have provided extremely helpful resources and guides. The ones listed below are some that we found useful during our research in the creation of this guide, but it should in no way be considered as an exhaustive list.

Online Safety Courses and Resources

Digital Hygiene Course

From TrollBusters, this course offers 16 free and publicly available modules to be taken at your own convenience, lasting about 5-10 minutes each, that have the goal of preventing digital harassment before it happens and focus on the following topics:

- Removing public data
- Privacy protection on domain names
- Https everywhere
- Anonymous “Tor” cloak or VPN
- Prepare for a DDoS attack
- Two-step verification
- Privacy plug-ins/cookies
- Third-party permissions
- Image “hidden pixels”
- Links and attachments
- Install patches and updates
- Use a password manager/strong password
- Strengthen security questions
- Encrypt hard drive/backup data
- Click to play
- Use end-to-end encryption

Keep it Private

This course is developed by the International Women’s Media Fund and geared specifically towards women journalists. It focuses on privacy online and the consideration of what information to share publicly in order to best protect yourself and your family. The course is offered for free on Totem and consists of interactive courses on various aspects of digital security and privacy. The course overall takes about an hour and a half and covers understanding what data is best kept private and why, learning how to better protect your online privacy, being able to speak with family and friends about online harassment, and gaining practical tips for being more secure online.

Right to Be (formerly Hollaback) Bystander Intervention Trainings

Provides free and customized anti-harassment trainings

- **Distract, Delegate, Document, Delay, and Direct**
- What to do when you experience online abuse training

Tall Poppy

Tall Poppy is an app for corporations to help to safeguard their employees' digital safety by providing threat assessment, incident response, software app and training, support and personal digital safety management, and digital security measures.

Know Your Trolls

This training is also developed by IWMF for women journalists and offered for free via Totem. The goal of this training is to help journalists identify the abuse they are receiving online and who may be behind it as well as offer some key strategies that may help journalists to be better prepared. It takes about an hour and covers recognizing types of online abusers and how they work together, becoming more familiar with some of the tactics online abusers use, and being equipped with some key strategies for dealing with abuse.

Knight Center - **Online Harassment: Strategies for Journalists' Defense**

James W. Foley Legacy Foundation - **Journalism Safety Modules**

- Readings and discussions around online harassment in the U.S. context for journalism students
- Chapter 9

Free Press Unlimited - **Safety Training for Female Journalists**

Electronic Frontier Foundation - **Lessons in security they may not teach you in your j-school**

CREA

Indian feminist human rights organization with online training programs that focus on feminist policy and activism including gender-based violence prevention and online safety

Cyberwomen

Digital protection training geared towards both professional trainers and those who want to learn how to train others on their digital protection - aimed at training human rights defenders and journalists working in high-risk environments

Toolkits

Fix the Glitch Toolkit

This toolkit provides a conversation guide, informed by experts, on hosting a group conversation about online gender-based violence in your communities.

Fix the Glitch Toolkit 2.0 - Helping to End Online Gender Based Violence for Black Women

This follow-up toolkit, also created by Glitch, aims to focus particularly on mitigating harm against Black women online, who have been shown to be attacked online at disproportionate rates to their white counterparts. One study from Amnesty International showed that Black women were 84% more likely than white women to be mentioned in abusive or problematic tweets. This toolkit is aimed towards Black women and bystanders looking to end online gender-based violence against Black women and features a conversation guide for ending online gender-based violence within your communities and networks.

The Intersectionality and Cybersecurity Toolkit

This toolkit looks at how to best address cybersecurity in the UK to prioritize human rights, equality, and transparency. Its main goals are to introduce intersectionality, reconceptualize cybersecurity's purpose as protecting people, provide pathways for actioning an intersectional lens in cybersecurity, and share complimentary resources for further learning.

Helplines/Networks/Reporting Mechanisms

HeartMob

By Right To Be - helps with documenting abuse as well as providing a community for messages of support

Vita Activa

Spanish language - support to women journalists, activists and women's rights defenders who are facing online violence when they reach out

Hamara Internet

In Pakistan, goal of empowering women and girls to thrive in digital spaces and engage safely/defend themselves

JSafe App

Allows women to document attacks and provides resources

Women's Reporting Point

Place for women journalists to report harassment and have their reports handled by women staff

Games and Online Harassment Hotline

For journalists experiencing online harassment

Committee to Protect Journalists **emergency help regional contacts**

Journalists in Distress Network

Lists media freedom organizations which provide direct assistance to journalists and media workers who are at risk because of their work

Legal Resources

Types of Online Harassment That Can Be Taken To Court

This resource from the Ontheline Platform for Newsrooms breaks down causes of legal action that may be available within local contexts. However, each legal system is different, so often this needs to be handled on a case-to-case basis.

Legal Considerations

This guide from PEN America walks through and provides resources for beginning to understand your legal rights around online harassment in the United States.

HateAid

HateAid is a German advice center for fighting online harassment, including an app that allows you to report online violence and receive personalized advice.

#SHE PERSISTED

A Digital Resilience Toolkit for Women in Politics

Persisting and Fighting Back Against Misogyny and Digital Platforms' Failures