WORLD LIBERTY CONGRESS · PLAYBOOK FOR LIBERTY

Online Defamation and Smear Campaigns: How to Respond

A practical guide for WLC activists facing coordinated online attacks, false accusations, impersonation, doxxing, and regime-linked reputation warfare.

Purpose: help activists respond with evidence, discipline, safety, and narrative strength rather than panic or endless reaction.

Core idea: The goal of online defamation is not only to insult you. It is to isolate you, exhaust you, make allies hesitate, make donors nervous, divide the movement, and prepare the ground for legal or physical repression.

1. Identify the type of attack

Task	Why it matters	What to do now
Smear narrative	Claims you are corrupt, foreign-controlled, immoral, extremist, or "fake opposition."	Track repeated phrases and identify who amplifies them.
Doxxing	Publishes private address, phone, family details, travel plans, or documents.	Treat as a safety incident; preserve evidence; report immediately.
Impersonation	Fake account uses your name, photo, logo, or organization identity.	Report to platforms; warn contacts; publish a verification notice.
Gendered or sexualized abuse	Targets women, LGBTQ+ activists, or family roles with humiliation and threats.	Escalate as high-risk abuse; document; protect mental health and physical safety.
Deepfake or manipulated media	Uses altered images, voice, video, or fake screenshots.	Preserve original; seek technical review; respond with evidence, not outrage.
Bot or troll swarm	Many accounts repeat the same narrative to create false consensus.	Do not debate each account; respond once through trusted channels.
Legal intimidation online	Threats of lawsuits, "treason" accusations, criminal complaints, or extradition claims.	Consult counsel; preserve posts; avoid emotional statements.

2. The first rule: do not chase every lie

Authoritarian propaganda often works by forcing activists into permanent defense. If every falsehood becomes an emergency, the regime controls your calendar. The movement must decide which attacks to ignore, which to document quietly, and which to answer publicly.

Decision filter: Respond publicly only when the attack threatens safety, credibility with key audiences, legal standing, donor trust, coalition unity, or the security of others.

3. The 24-hour response method

1. Pause and assign one coordinator

Do not let ten people respond emotionally. Choose one person to coordinate evidence, messaging, platform reports, and ally outreach.

2. Assess safety

Ask whether the attack includes threats, addresses, family details, travel information, or calls for violence. If yes, treat it as a security incident, not only a communications problem.

3. Capture evidence

Save URLs, screenshots, account handles, timestamps, follower counts, and repeated language. Use a shared evidence log. Do not rely on memory.

4. Classify the attack

Is this a rumor, coordinated smear, doxxing, impersonation, manipulated media, or legal threat? Different attacks require different responses.

5. Choose the response level

Level 1: monitor quietly. Level 2: platform report. Level 3: private ally briefing. Level 4: public statement. Level 5: legal/security escalation.

6. Respond with one clear message

Do not argue with trolls. Publish a short, factual correction through verified channels if necessary, then return to your mission.

7. Support the person targeted

Online abuse can produce fear, shame, exhaustion, and isolation. Check on the person. Rotate public duties if needed.

4. How to write a disciplined public response

A good response is short, calm, factual, and mission-centered. It should not repeat every false allegation in detail. It should deny the core falsehood, explain the pattern, and return to the work.

Weak response	Stronger response
“They are lying. They are disgusting. Everyone knows who pays them.”	“A coordinated smear campaign is circulating false claims about our work. Our position is clear: our organization serves democratic values, political prisoners, and families affected by repression. We will not be distracted from that mission.”
“Here are twenty screenshots of every insult they posted.”	“We have documented the accounts involved and will report threats and impersonation through the appropriate channels.”
“Our enemies are traitors.”	“We reject dehumanizing language. Our movement defends dignity and truth, even under attack.”

5. The evidence log template

Date/time	Platform	Account/URL	Type of attack	Risk level	Action taken

Keep this log in a secure shared folder with limited access. Do not include unnecessary personal information. Export copies periodically in case platforms remove content.

6. Protect accounts and channels

- Turn on two-factor authentication for email, social media, cloud storage, and messaging apps.
- Use password managers and unique passwords for every account.
- Check account recovery emails and phone numbers; remove old numbers or unsafe addresses.
- Limit who can post from official accounts.
- Prepare backup admins for official pages.
- Use verified channels to announce authentic statements.
- Do not share login credentials through chat apps.
- Create an impersonation reporting folder with IDs, logos, and official URLs ready.

7. Counter the narrative, not every attacker

Regime-linked smear campaigns often use predictable narratives: foreign agent, corrupt activist, red-carpet dissident, anti-family, anti-religion, extremist, traitor, fake victim, or donor puppet. The best response is to build a durable counter-narrative before the attack arrives.

- Show community roots: who do you serve?
- Show transparency where safe: what do you do, how are decisions made, and what impact is documented?
- Show human benefit: prisoners supported, families helped, youth trained, abuses documented.
- Show civic patriotism: defending democracy is defending the country, not serving foreigners.
- Use trusted voices: beneficiaries, families, religious leaders, teachers, doctors, artists, local community members.
- Prepare a “what we do” one-pager before smear campaigns begin.

8. How to support a targeted activist

- Ask what they need before posting on their behalf.
- Help document the attack so they do not have to keep rereading abuse.
- Rotate public-facing duties if they need rest.
- Offer legal, digital security, and psychosocial referrals.
- Do not pressure them to be brave in public if they need privacy.
- Check again after the online storm fades. Harm often lasts longer than the news cycle.

9. What WLC teams should prepare in advance

- A list of official accounts and verified spokespersons.
- A platform reporting guide for impersonation, doxxing, and threats.
- A rapid-response small team: evidence, safety, messaging, legal/digital referral.
- A pre-approved mission statement explaining WLC values and local legitimacy.
- A short “false narratives we expect” document with prepared rebuttals.
- A trusted journalist list for serious cases only.
- A care protocol for activists facing gendered, racist, religious, or family-based abuse.

10. Common mistakes to avoid

- Responding to every troll and giving the campaign more reach.
- Using angry language that makes the movement look unstable.
- Sharing screenshots that include private data of victims or families.
- Publishing unverified claims about who is behind the attack.
- Treating online abuse as “not real” when it includes threats or doxxing.
- Leaving the targeted activist isolated.
- Letting smear campaigns define the movement’s message for weeks.

Selected practical resources

Use these resources as starting points. Always adapt them to local risk, language, and legal context. Do not upload sensitive case material to any platform unless the security protocol has been approved.

- **PEN America: Combatting Online Abuse:** Practical guidance for journalists and writers facing online abuse and threats. Link
- **Online Violence Response Hub:** Support resources and courses for people targeted by online violence. Link
- **TrollBusters:** Support and guidance for journalists targeted by online abuse. Link
- **Access Now Digital Security Helpline:** Technical assistance for civil society and human rights defenders. Link
- **EFF Surveillance Self-Defense:** Guides for threat modeling and account protection. Link
- **Security in-a-Box:** Digital security guide for activists and human rights defenders. Link

Final reminder

Remember: A smear campaign wants to drag you into confusion. Your response should restore clarity: protect the person, preserve evidence, answer only what matters, and return to the mission.