HuMENA For Human Rights and Civic Engagement
HuMENA pour les Droits de l'Homme et l'Engagement Civique
هيـومينـا لحقـوق الإنسـان والمشاركـة المدنيـة

POCKET COMPANION · 2026 EDITION

# Public Sphere Safety Handbook

Digital violence in Lebanon's public sphere is a deliberate tactic — used to punish visibility, deter participation, enforce self-censorship, and narrow civic space.

This Handbook is the pocket-sized companion to the Public Sphere Safety Kit. Recognise the attack. Triage the risk. Act in the first 24–72 hours.

For Women Human Rights Defenders, women in public and civic life, candidates, LGBTQI+ defenders, allies, community organisers, and anyone who may witness digital attacks in Lebanon's public sphere.

Grounded in the lived experiences of WHRDs, women civic actors, and LGBTQI+ defenders in Lebanon, and validated through participatory workshops with those communities.


info@humena.org · lebanon@humena.org
www.humena.org

In partnership with

INNOVATION FOR CHANGE MIDDLE EAST & NORTH AFRICA · CIVICUS · Digital Democracy Initiative

NAVIGATION

# How to use this Handbook

Read the first page under pressure; use the rest as a quick reference.
Recognise the attack, triage the risk, then act in the order set out here.


- If you can only read one page — 03
- 01 Recognising attacks — 04
- 02 Rapid risk identification — 05
- 03 Risk scoring matrix — 06
- 04 First 24–72 hours response flow — 07
- Helplines & resources — 09
- Want the full guidance? · About HuMENA — 10


★ In an active incident, go straight to page 03 — **"If you can only read one page."** Everything else can wait.

IF YOU CAN ONLY READ ONE PAGE

# Read this one.

This Handbook is the condensed pocket companion to the full Public Sphere Safety Kit. It exists to help you act quickly under pressure. For deeper guidance, see the Kit.

**ACT NOW** **The first three actions when an attack begins**

1. **PAUSE**
   Don't respond publicly. Don't engage. Don't delete accounts or content. Step away from the screen for a minute before deciding the next step.

2. **DOCUMENT**
   Screenshot abusive content (username, date, time, platform visible). Save URLs. Note account details. Store everything in a secure folder, organised by date. If content can't be screenshotted, photograph it with a second device.

3. **REACH TRUSTED SUPPORT**
   Tell one person you trust. Ask for specific help — monitoring, evidence collection, or communications. If family or partner is part of the risk, choose someone outside that circle. LGBTQI+ users facing outing: contact Helem or MOSAIC first — not the ISF.

WHEN IN DOUBT

**If unsure about risk level: treat as high risk and move to protective action.**

> "Pause. Document.
> Reach trusted support
> — in that order, every time."

01 KNOW THE FORM

# Recognising attacks

Six common forms of online violence in Lebanon, the patterns that distinguish each, and where they tend to lead. Knowing what kind of attack you face is the first step in choosing the right response.

| TYPE | WHAT IT LOOKS LIKE |
|---|---|
| **Technology-Facilitated Gender-Based Violence (TFGBV)** | Degrading or sexualised language, threats, humiliation, and content shared to shame or silence someone on the basis of gender or identity. |
| **Doxxing** | Private information — home address, phone number, workplace, family details — exposed online without consent, often to enable offline threats. |
| **Outing** | Non-consensual disclosure of sexual orientation, gender identity, or other sensitive personal information. Carries immediate legal, social, and physical risks in Lebanon. |
| **Impersonation** | Fake accounts, fabricated statements, manipulated screenshots, or false attribution designed to damage reputation and provoke harassment. |
| **Coordinated harassment** | Organised, simultaneous abuse from multiple accounts or networks. Recognisable by similar phrasing, common timing, and cross-platform spread. |
| **Non-consensual intimate images (NCII) & deepfakes** | Sharing or threatening to share real or AI-generated sexual content. Use StopNCII.org to pre-emptively block known images; consult Legal Agenda or ABAAD before any formal complaint involving intimate evidence. |

These attacks **rarely happen in isolation**. They overlap, reinforce one another, and escalate over time.

02 ⚠ ASSESS BEFORE REACTING

# Rapid risk identification

Not every attack carries the same urgency. Assess quickly, before reacting. Risk levels are not fixed; reassess as the situation evolves. When in doubt, treat the situation as high risk.

## 2.1 Risk levels at a glance

**✓ LOW**

Isolated incident, limited visibility, no personal data exposed, no threats, no signs of coordination.

**! MEDIUM**

Sustained or expanding attacks, content spreading across platforms, early signs of coordination, partial exposure, threats emerging.

**⚠ HIGH**

Doxxing, direct threats of physical or sexual violence, viral coordinated harassment, outing threats, attacks extending to family or colleagues, signs of offline harm.

**OVERRIDE — Threats, doxxing, or any offline risk treat as HIGH regardless of total score.**

## 2.2 Response by level

**LOW** Monitor. Document. Block aggressor. Tighten privacy settings. Inform one trusted person.

**MEDIUM** Document patterns (not just single posts). Limit public exposure. Avoid amplifying harmful content. Activate support network.

**HIGH** Stop real-time posting. Turn off location sharing. Contact legal or security support through trusted civil society organisations (see Helplines page). LGBTQI+ users: do **NOT** contact the ISF before consulting Helem, MOSAIC, or Legal Agenda — Article 534 of the Lebanese Penal Code has been used to detain LGBTQI+ individuals based on digital evidence shared in good faith during such complaints.

03 SCORE IT

# Risk scoring matrix

Score each indicator: 0 for Low, 1 for Medium, 2 for High. Sum the scores and refer to the interpretation below. If any "override" condition applies — threats, doxxing, offline risk — treat as HIGH regardless of total.

| INDICATOR | LOW (0) | MEDIUM (1) | HIGH (2) |
|---|---|---|---|
| **Attack type** | Single, low-level | Repeated or overlapping | Multiple types, coordinated |
| **Visibility / spread** | Private or limited | Public or growing | Viral, cross-platform |
| **Doxxing / NCII / deepfakes** | No personal data | Partial exposure | Sensitive data exposed |
| **Coordination** | None | Emerging patterns | Coordinated, same messaging |
| **Threats** | None | Implied or indirect | Direct, violence or sexual |
| **Escalation** | Stable | Increasing | Rapid surge |
| **Impact on others** | Only target | Mentioned | Family or colleagues targeted |
| **Offline risk** | None | Indirect references | Tracking, contact, proximity |
| **Source of attack** | Unknown individual | Multiple suspicious accounts | Partner, organised actors, networks |
| **NCII** | No | No | Yes |
| **IPV** | No | No | Yes |
| **TOTAL / 20** | *Sum every indicator, then read the interpretation below.* | | |

## SCORE INTERPRETATION

**0–6 LOW**
Limited exposure, no immediate threat. Monitor and apply basic measures.

**7–12 MEDIUM**
Situation is escalating. Respond and contain to prevent further escalation.

**13–20 HIGH**
Serious risk of digital and physical harm. Immediate protective action; seek support.

04

ACT IN ORDER

# First 24–72 hours response flow

The first hours after an attack shape how it evolves. The sequence below increases safety and preserves your options. Each step reinforces the next; do them in order if you can.

1

## PAUSE AND ASSESS

Don't respond publicly. Don't engage with aggressors while distressed. Identify the type of attack and whether it's isolated or coordinated. Use the risk triage on the previous page. Don't delete accounts, messages, or content — preserve everything.

2

## DOCUMENT

Screenshot all abusive content (username, date, time, platform visible in each shot). Save URLs. Note account details. Log dates and times of each escalation point. If content can't be screenshotted, photograph with a second device. Store securely and chronologically. Ask a trusted person to assist so you're not repeatedly exposed to harmful material. Document even if you don't plan to report yet.

3

## SECURE YOUR ACCOUNTS

Change passwords on all key accounts. Enable two-factor authentication. Log out of all active browser sessions remotely. Restrict who can contact, tag, or message you across platforms. Disable location sharing and geotagging. Switch sensitive communication to Signal or another end-to-end encrypted channel.

→ Steps **4 to 6** — activating support, choosing a response path, and reassessing — continue on the next page.

CONTINUED **First 24–72 hours response flow**

### 4 Activate trusted support

Tell at least one trusted person. Ask for specific help — monitoring content, collecting evidence, managing communications. Contact a digital security organisation (SMEX, Access Now) if account compromise is suspected. Contact legal aid (Legal Agenda, CLDH, ABAAD) if threats, doxxing, or outing are involved. Seek psychological support if distress is significant. State institutions (including the ISF) should not be approached without prior consultation with a civil society organisation.

### 5 Choose a response path

Monitor without engaging (low risk): document, block, report to platforms, reassess regularly. Escalate (medium/high risk): inform trusted people, seek legal and digital security support; LGBTQI+ users must consult Helem, MOSAIC, or Legal Agenda before any ISF contact. Public clarification: only where impersonation, false allegations, or disinformation require correction. Keep it factual, brief, and non-engaging.

### 6 Reassess continuously

Response paths are not fixed. Situations escalate and de-escalate quickly during politically sensitive periods. Update your strategy as conditions change.

**NOTE ON "TRUSTED"**

Where “trusted” appears in this Handbook, read it as **“chosen trusted contacts”** if your family or partner is part of the risk. For attacks originating from family or intimate partners, refer to **ABAAD (+961 81 788 178)** or **KAFA (+961 3 018 019)** , not general digital security organisations.

VERIFIED CONTACTS

# Helplines & resources

Verify contact details before urgent use — Lebanon's operating environment changes quickly. Updates: **lebanon@humena.org**

## LEGAL AND RIGHTS

**Legal Agenda**
**+961 1 383 606**
info@legal-agenda.com

**CLDH (Lebanese Center for Human Rights)**
**+961 1 24 00 23**

**Front Line Defenders** (Dublin, 24h)
**+353 1 21 00 489**

## LGBTQI+

**Helem helpline**
**+961 81 478 450**
info@helem.net

**MOSAIC helpline**
**+961 76 945 445**

**Marsa Sexual Health Centre**
**+961 1 565 522**

## WOMEN & GENDER-BASED VIOLENCE

**ABAAD safe line** (24/7)
**+961 81 788 178**

**KAFA** (intimate partner abuse)
**+961 3 018 019**

**RDFL**
**+961 71 500 808**

## DIGITAL SECURITY

**SMEX helpdesk**
**+961 81 633 133**
helpdesk@smex.org

**Access Now Digital Security Helpline**
(24/7, Arabic-capable)
help@accessnow.org

## PSYCHOSOCIAL

**Embrace lifeline** (24/7)
**1564**

GO DEEPER

# Want the full guidance?

This Handbook is the condensed pocket version.
The full Public Sphere Safety Kit covers everything not in here:

- Safer participation strategies — how to adjust visibility without full withdrawal from public life;
- Standards for page admins and community moderators;
- Targeting of women journalists and diaspora / cross-border attacks;
- Pre-incident preparedness checklists;
- A glossary, references, and further reading.
- Guidance for allies, friends, and colleagues — what to do and what to avoid;
- What others must do — platforms, parties, employers, donors;
- Platform reporting guidance, including Telegram-specific notes;
- Full support pathways and a verified resource directory;

Find the Kit at **www.humena.org** or write to **lebanon@humena.org** for a copy.

## ABOUT HUMENA

HuMENA for Human Rights and Civic Engagement is an independent, non-profit organization that works to protect and expand civic space in the Middle East and North Africa. Based in Brussels with a regional office in Beirut, it supports human rights defenders and civil society actors, especially those in exile and the diaspora, through advocacy, research, and training.

Its work spans the core civic freedoms of expression, peaceful assembly, and association, both offline and online. HuMENA helps individuals and movements organize safely and sustain their activism under repression.

The organization works closely with women, refugees, LGBTQI+ people, and other marginalized communities, and builds gender equity and social justice into its programs. Documentation, advocacy, and artivism are central to its approach.

HuMENA For Human Rights and Civic Engagement
HuMENA pour les Droits de l'Homme et l'Engagement Civique
هيـومينـا لحقـوق الإنسـان والمشاركـة المدنيـة

**Public Sphere Safety Handbook** — HuMENA 2026

# RECOGNISE. TRIAGE. ACT IN THE FIRST 24–72 HOURS.

The pocket companion to the Public Sphere Safety Kit — built with and for the communities most exposed in Lebanon's public sphere.


CONTACT

info@humena.org · lebanon@humena.org

www.humena.org


**In partnership with**

Innovation for Change Middle East & North Africa · CIVICUS · Digital Democracy Initiative