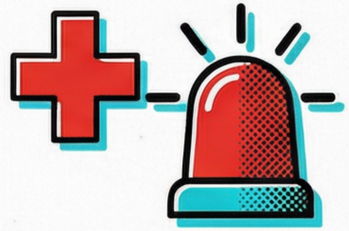
Womenatrix Survival Kit

North Africa Operational Protocol for Digital Violence

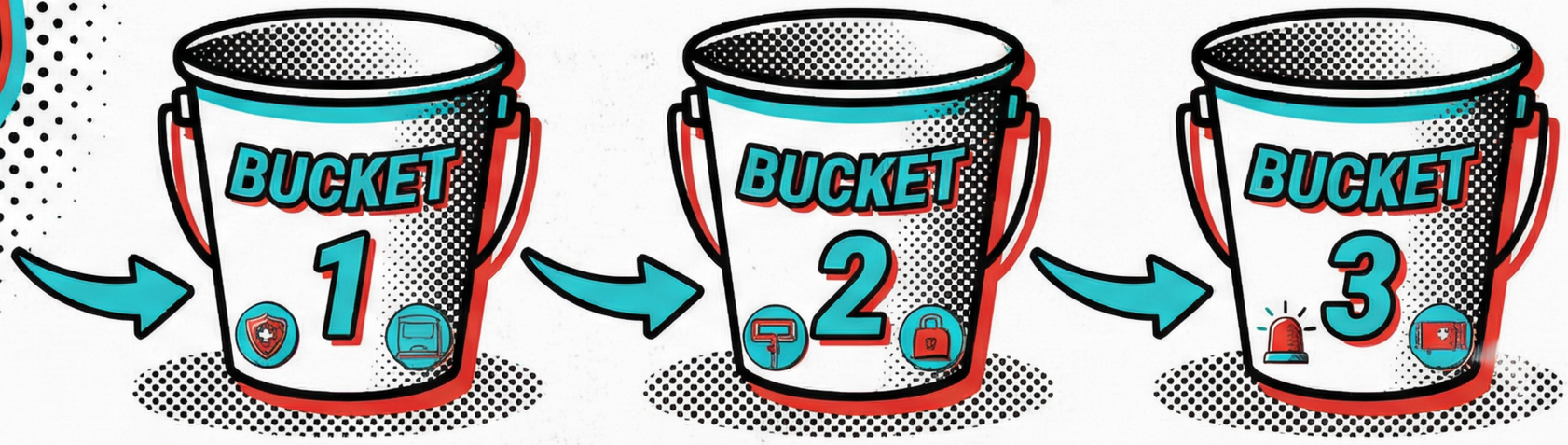
INTRODUCTION: THE TRIAGE MAP

Do not read this guide from start to finish.



Digital violence creates chaos. Your brain is likely overwhelmed. To survive this, you must treat your situation like a medical emergency: identify the urgency and go immediately to the right section.

We have organized this manual into three operational buckets. Find your current status below and skip to that section.



WOMENATRIX SURVIVAL KIT – NORTH AFRICA PROTOCOL

THE PANIC BUTTON
(Crisis Response)

Status: "It is happening right now."

Signs: You just found a leaked image; you are being blackmailed; you are receiving threats; your account is locked; you are being doxxed.

Goal: Stop the bleeding. Secure the perimeter. Preserve evidence.

Go to: [PART 1: STOP THE BLEEDING]

THE SHIELD
(Prevention)

Status: "I am safe, but I am worried."

Signs: You are a journalist, activist, or content creator; you see others being attacked; you suspect someone is watching your account; you want to separate your identity from your work.

Goal: Build the fortress. Hardize accounts. Clean data.

Go to: [PART 2: BUILD THE FORTRESS]

THE RECOVERY
(Aftermath)

Status: "The attack happened. Now what?"

Signs: The immediate threat has paused; you are deciding whether to go to the police; you are dealing with burnout, fear, or reputation damage.

Goal: Fight back (institutionally) and Heal the human (psychologically).

Go to: [PART 3: FIGHT BACK] or [PART 4: HEAL THE HUMAN]

CRITICAL WARNING: THE REGIONAL REALITY – NORTH AFRICA PROTOCOL

Read this before acting. This guide distinguishes between Technical Tools and Legal Tools.

Technical Tools are Universal

Two-Factor Authentication (2FA), encryption, and platform reporting work the same way in Tunis as they do in Cairo or Algiers. These are generally safe to use.

Legal Tools are Local & Dangerous

Laws change at the border. A strategy that works in Tunisia can get you arrested in Egypt or Mauritania.

The "Double-Edged Sword" Risk Map: Before approaching any police station or court, check your specific country risk card below.

Tunisia:

Tunisia: Decree 54 (Article 24): Broad provisions on "false news" create a high risk of counter-prosecution for public posts.

Safety Rule: Do not use political speech in your complaint unless necessary. Use Law 58 specialized units.

Egypt:

Egypt: "Family Values" (Art. 25): Survivors of sextortion or harassment can be arrested for "violating family values" or "inciting debauchery."

Safety Rule: NEVER go to the police alone if the content involves your private life/body. Contact a trusted lawyer first.

Morocco:

Morocco: Article 490: Reporting sexual blackmail can lead to prosecution for "sexual relations outside marriage."

Safety Rule: Use the anonymous E-Blagh portal. Do not confess to consensual relationships in police reports.

Mauritania:

Mauritania: Zina Laws: Rape or sextortion survivors risk being charged with adultery (Zina).

Safety Rule: NEVER enter a police station without an NGO escort (e.g., AMSME).

Sudan / Libya:

Sudan / Libya: Militia Weaponization: Digital data is used by armed groups for targeting and abduction.

Safety Rule: Avoid standard police channels. Use trusted community networks (ERRs) or international hotlines.

Algeria:

Algeria: Internet Shutdowns: Frequent state-imposed blackouts.

Safety Rule: Prepare offline backups of evidence and codes.

The Golden Rule of North Africa: "Tech First, Law Second."

Always secure your accounts, block the aggressor, and preserve evidence (**Tech**) before you decide to engage with the state (**Law**).
The platform algorithm is indifferent to you, but the state may be hostile.

PART 1: STOP THE BLEEDING

(Immediate Crisis Tools — North Africa Edition)

AUDIENCE: UNDER ATTACK

You are currently under attack. Your image has leaked, you are being threatened, or you have lost access to your accounts.

GOAL: STABILIZE & SECURE

Stabilize your safety, secure your data, and stop the damage from spreading.

1.1 The "First 30 Minutes" Protocol

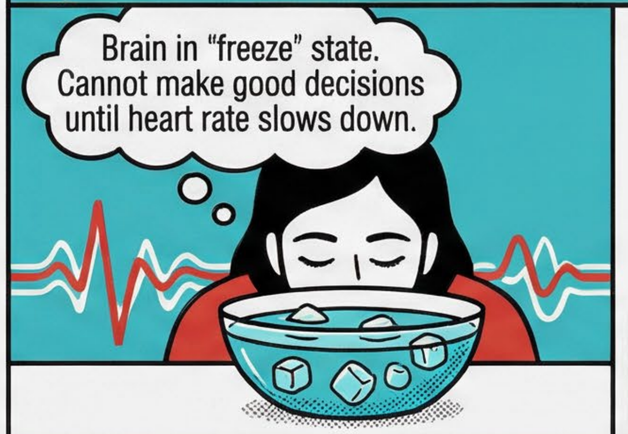
Do not try to solve the whole problem right now. Follow this timeline strictly.

A) Physical Safety Check — Decision Tree

START: ASSESS THREAT SOURCE

- **IF** anonymous, general, or stranger abroad: → **ACTION:** Stay where you are. Lock doors. Do not leave safe space.
- **IF** mentions current, real-time location (e.g., "I see you at [Cafe Name]"): → **ACTION:** Relocate immediately to public place or trusted friend. Vary route.
- **IF** home address posted publicly (Doxxing): → **ACTION:** Leave home immediately if possible. Go to friend or family not tagged.

B) Somatic Reset — Mammalian Diving Reflex



- **What to do:** Fill a bowl with cold water (or use ice pack). Hold breath and submerge face (or hold ice to upper cheeks/under eyes) for 30 seconds.
- **Why:** Forces nervous system to lower heart rate immediately.

⚠ **Safety Warning:** Do not do this if you have known heart condition.

C) The Digital Freeze

- **Stop:** Put phone in another room or hand it to a friend.
- **Timer:** Set a timer for 15 minutes.
- **Rule:** Forbidden from looking at screen until timer rings.

D) Immediate Perimeter Lockdown

Do this immediately, even if you plan to delete or report accounts later.

- ☑ **Go Private:** Switch profiles on Instagram, TikTok, and X to "Private" or "Protected".
- ☑ **Kill Sessions:** Go to Settings > Security > Login Activity (on FB/IG/Google). Select "Log Out of All Other Sessions." Kicks out anyone currently in your account.
- ☑ **Change Critical Passwords:** Change your Email password first. If they have your email, they can take everything else.
- ☑ **Turn off DMs:** Restrict who can message you to "Friends only" or "No one".

1.2 The NCII & Sextortion Breaker

Use this if intimate images/videos are involved.

A) StopNCII.org Guide

- **When to use:** If you have the image/video file, or if you are threatened that it will be posted.
- **How it works:** It creates a "digital fingerprint" (hash) of the image on your device. It sends only the fingerprint to companies, not the image itself.
- **Website:** https://stopncii.org https://stopncii.org →
- **What it does NOT do:** It cannot remove images from Telegram, WhatsApp, or random websites. It only protects participating platforms.

B) The "DO NOT PAY" Script

If a blackmailer demands money, crypto, or more photos:

- **Rule: NEVER PAY.** Payment marks you as a "payer" and they will sell your contact info to other blackmailers. It never ends.
- **Rule: NEVER ARGUE.** Do not beg or threaten. Silence is your best weapon.

- **The Protocol:** 1. Screenshot the threat (capture the User ID/Number). 2. Block the user. 3. Deactivate your account temporarily (do not delete).

C) Copyright Takedown Method

If the image/video was taken by YOU (a selfie or solo video), you own the copyright. Platforms remove copyright violations faster than harassment.

- **When to use:** Only if you held the camera.

- ☑ **When to use:** Only if you held the camera.
- ☑ **Action:** Find the "Report" form on the platform. Select "Intellectual Property Violation" or "Copyright".
- ☑ **Claim:** "I am the copyright holder of this image. It is being used without my permission."

1.3 Crisis Communication Templates

Do not try to solve the whole problem right now. Follow this timeline strictly.

A) Message to Platform (Universal)

Use this text when reporting content. It avoids admitting to relationships or providing details that could be used against you legally in North Africa.

Language	Copy/Paste Template — REPORT
English	I am reporting this content for non-consensual sharing of private intimate images. This is a severe violation of my privacy and a direct threat to my safety. Please escalate to a human reviewer immediately.
Arabic	أقوم بالإبلاغ عن هذا المحتوى بسبب مشاركة صور خاصة دون موافقة. يعد هذا انتهاكًا خطيرًا لخصوصيتي وتهديدًا مباشرًا لسلامتي. يرجى تصعيد الأمر للمراجعة البشرية فورا.
French	Je signale ce contenu pour partage non consensuel d'images intimes privées. Il s'agit d'une violation grave de ma vie privée et d'une menace directe pour ma sécurité. Veuillez transmettre ce signalement à un examinateur humain immédiatement.

B) Message to "Support Squad"

Send this to 1–2 trusted people (friend, colleague). Do not face this alone.

I am facing a digital attack/blackmail right now. I am physically safe, but I am overwhelmed. I need you to handle two things so I don't have to look at the screen:

1. Screenshot/Document the abuse.
2. Report the account/posts.

Please do not ask me for details right now. Just help me block the noise.

C) Regional Emergency Mentions

Use these numbers/portals for immediate help.

WARNING: See Section 1.4 regarding legal risks:

Tunisia: 1899 (Green Line - Govt) or ATFD (+216 71 890 011 - NGO)

Morocco: E-Blagh Portal (Anonymous reporting) or UAF/Centre Annajda (05 37 70 09 64).

Egypt: 15115 (National Council for Women).

Mauritania: 1013 (AMSME - NGO). Do not call police alone.

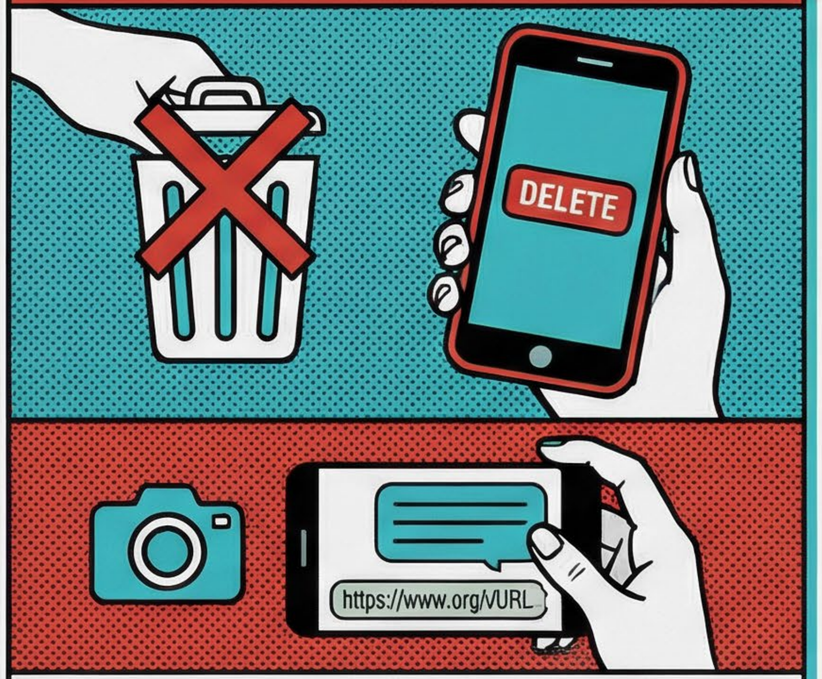
Sudan: Contact trusted Emergency Response Rooms (ERR) via Signal. Avoid official channels.

Libya: 1417 (UNFPA Hotline). Avoid militias/police.

Algeria: 0560 100 105 (Réseau Wassila).

1.4 The "DO NOT" List — Panic Pitfalls

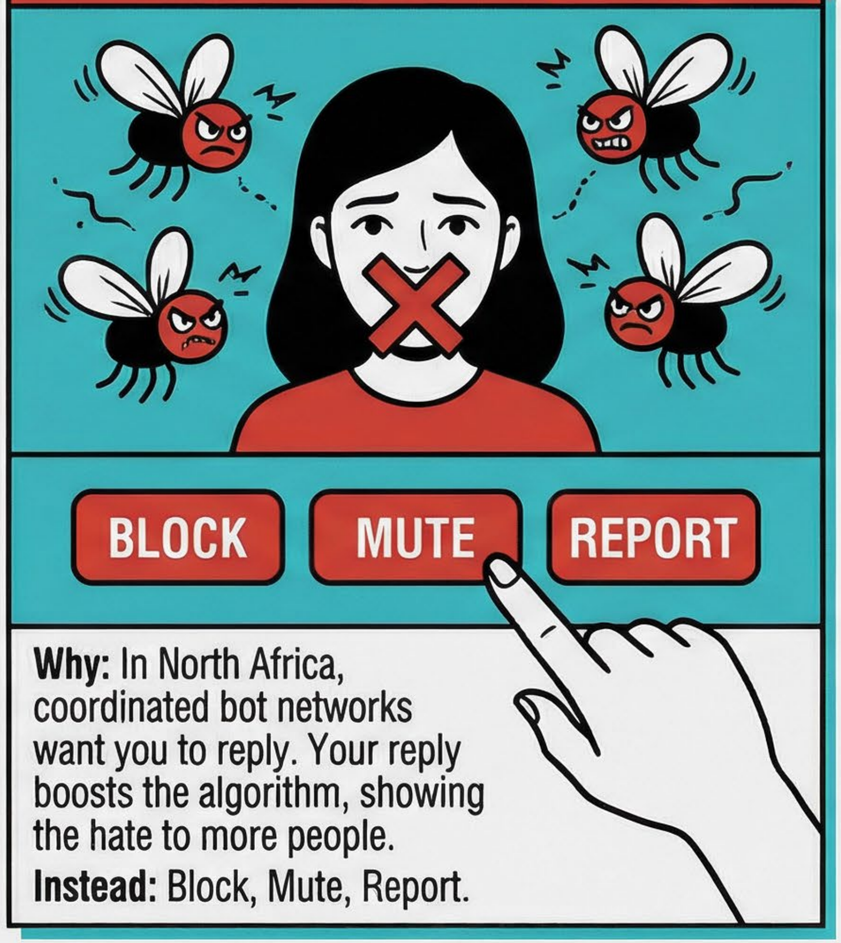
DO NOT Delete Evidence.



Why: If you delete the messages or posts sent to you, you destroy the only proof legal teams need to help you later.

Instead: Archive chats, take screenshots (with URLs), or deactivate the account.

DO NOT Engage with "Electronic Flies" (Trolls).



Why: In North Africa, coordinated bot networks want you to reply. Your reply boosts the algorithm, showing the hate to more people.

Instead: Block, Mute, Report.

DO NOT Confess to Relationships in Police Reports.

Why: In Egypt (Article 25), Morocco (Article 490), Mauritania, and Sudan, if you tell police "my boyfriend posted this," you risk being charged with Zina, "Debauchery," or "Crimes against Family Values".

Instead: Stick to the technical crime: "This person is using digital means to harass/extort me." Consult a lawyer/NGO before speaking to police.

PART 2: BUILD THE FORTRESS

(Prevention — Tailored for Regional Infrastructure)

WHEN TO USE THIS SECTION

"THIS SECTION IS FOR WHEN YOU ARE SAFE, NOT WHEN YOU ARE UNDER ATTACK."

THE GOAL: REDUCE YOUR ATTACK SURFACE

THE GOAL IS TO **REDUCE YOUR 'ATTACK SURFACE'**—THE AMOUNT OF INFORMATION AVAILABLE FOR ABUSERS OR AUTHORITIES TO USE AGAINST YOU."

2.1 The Fortress Audit

Time required: ~20 minutes.

A) Password & Manager Check

Using the same password everywhere is the **single biggest risk.** If one site leaks, hackers try that password on your Facebook and email immediately.

The Solution: Use a Password Manager. This tool remembers your passwords for you, so you can use complex, impossible-to-guess codes for every account.

Bitwarden: (Cloud-based, easy to use across devices).

KeePassXC: (Offline, best for high-risk users who don't trust the cloud).

1. **Download** the app (Bitwarden or KeePassXC).
2. **Create ONE Strong Master Password.** This is the only password you need to memorize. Make it a "passphrase" of 4+ random words (e.g., Red-Tea-Sky-Walking-99) so it is long but easy to type.
3. **Write down your Recovery Key.** If you lose your Master Password, you lose everything. Write the recovery code on paper and hide it safe offline.

The "Big Three" Change: Do not try to change 100 passwords tonight. Change these three immediately using the generator in the app:

- ☐ **Primary Email** (Gmail/Outlook)
- ☐ **Main Social Media** (Facebook/Instagram)
- ☐ **Cloud Storage** (iCloud/Google Drive)

B) 2FA Migration (Critical)

Why SMS is Weak: In North Africa, 'SIM Swapping' is a risk where attackers trick telecom providers into moving your phone number to their SIM card. If your Two-Factor Authentication (2FA) codes come via SMS, the attacker gets them.

The Upgrade: App-Based Authentication. This generates codes on your device, independent of the mobile network.

Aegis (Android). **Raivo** (iOS). **Authy** or **Google Authenticator** (General use).

1. **Download the authenticator app.**
2. **Go to Settings:** On Facebook/Google, go to Security > Two-Factor Authentication.
3. **Select "Authentication App":** Scan the QR code provided by the site.
4. **Save Backup Codes:** The site will show you 8–10 "Backup Codes." Print these or write them down. If you lose your phone, these are the only way back in.
5. **Disable SMS:** Once the app is working, turn off the SMS option in the settings to close the security hole.

DO THIS FIRST: If you do nothing else tonight, enable 2FA on your WhatsApp and Facebook.

- **WhatsApp:** Settings > Account > Two-Step Verification > Enable.
- **Reason:** This prevents someone from stealing your account even if they steal your SIM card.

2.2 Data Scrubbing & Privacy

This is about cleaning up your digital footprint so you are harder to find or track.

A) The Google Scrub

Abusers and 'electronic flies' use details found on Google (old CVs, PDF lists) to find your home address or phone number.

1. **The Self-Search:**
   Open a browser in 'Incognito' mode. Search for:
   - Your Name
   - Your Name + 'Tunisia/Egypt/Morocco'
   - Your Phone Number
   - Your CIN/ID Number

2. **Identify Leaks:**
   Look for old university lists, government exam results, or job portals hosting your CV.

3. **Request Removal:**
   Google has a specific tool to remove 'Personally Identifiable Information' (PII).
   - **What they remove:** Phone numbers, physical addresses, ID numbers, images of signatures.
   - **What they refuse:** Public records, government websites, and news articles. Google removes the search result, but the page itself stays on the internet.

⚠ **Action:** Search 'Google Remove PII' and submit the URLs found in step 1.

B) Social Media Lockdown (Without Vanishing)

You can remain visible for activism or work while locking the 'back doors'.

Facebook Checklist:

- ☑ **Friend List:** Set to 'Only Me.' (Prevents abusers from mapping your network).
- ☑ **About Info:** Remove your phone number and address from the 'Contact and Basic Info' section.
- ☑ **Lock Profile:** If available in your region, enable 'Lock Profile' to restrict non-friends from downloading your full-size profile picture.
- ☑ **Active Sessions:** Go to Settings > Security and Login > Where you're logged in. Log out of all sessions you don't recognize immediately.

Instagram/TikTok Checklist:

- ☑ **Location Tags:** Stop tagging your current location in Stories. Post with a delay (after you leave the venue).
- ☑ **Mentions/Tags:** Change settings to 'People you follow' or 'No one' to prevent bot accounts from tagging you in spam/harassment attacks.
- ☑ **Story Visibility:** Use 'Close Friends' for personal content.
- ☑ **TikTok Privacy:** In Egypt, high visibility carries a risk of 'public morals' prosecution. Consider keeping your account private or strictly avoiding content that could be interpreted as 'incitement'.

2.3 Regional Device Hygiene (High-Risk Zones)

Warning: In conflict zones (Sudan) or authoritarian contexts (Egypt), your phone is a physical target.

A) The 'Checkpoint' Check (Egypt / Sudan)

Authorities and militias frequently search devices at checkpoints. They look for evidence of activism, foreign contact, or "immoral" content.

- ☐ **Audit Your Apps:** Remove apps that signal "activism" (specifically Signal and Twitter/X icons) if you are entering a hostile zone like RSF-controlled areas in Sudan.

- ☐ **Clean Your Gallery:** Move sensitive photos (protests, documentation of violence) to a "Hidden Folder" or, better yet, offload them to a secure cloud (Google Drive) and delete them from the device.

- ☐ **Messaging Hygiene:**
  - ☐ **Use Signal** with "Disappearing Messages" enabled (set to 1 week or less).
  - ☐ **Clear Call Logs:** If you contacted a hotline (like 1417 in Libya or 15115 in Egypt), delete the call log immediately.

- ☐ **Log Out:** Log out of Facebook and Gmail apps. A logged-out phone shows less information during a quick search.

- ☐ **RISK WARNING:** Do NOT use "Decoy Apps" (fake calculators that hide photos) at high-security checkpoints. Security officers know these apps. Finding one can make you look more suspicious than having an empty gallery.

B) The 'Shutdown' Prep (Algeria / Mauritania)

Governments in the region use internet shutdowns during exams or political unrest. You must prepare before the connection cuts.

- ☐ **Download a VPN:** Install it now. Once the internet is blocked or throttled, you cannot download one. Keep 2–3 different VPNs in case one is blocked.

- ☐ **Offline Backup Codes:** Ensure your 2FA backup codes (from Section 2.1) are saved as a screenshot or written down. You won't get SMS codes during a blackout.

- ☐ **Offline Contacts:** Write down key numbers (Emergency lawyers, family, trusted hotline) on physical paper.

- ☐ **Bridge Apps:** Download Tor Browser or request "Bridges" for Tor, which can sometimes bypass blocks when standard VPNs fail.

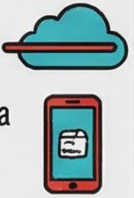
C) FemTech Audit (Sensitive Data)

In Morocco, Egypt, and Mauritania, data related to reproductive health (periods, pregnancy) can theoretically be weaponized in legal cases involving "Zina" (sex outside marriage) or abortion.

- ☐ **Review Apps:** Check any period-tracking or fertility apps installed.

- ☐ **Check Permissions:** Does the app track your Location? Disable it. There is no medical reason for a calendar to know where you are.

- ☐ **Data Storage:** If the app stores data in the cloud (online), assume it could be requested by authorities.
  - ☐ **Safer Alternative:** Use apps that store data locally on your device only (like "Euki" or similar privacy-focused tools).



- ☐ **Deleting:** Uninstalling the app does not delete your account data from the company's server. You must find the "Delete Account" button inside the settings first.

WOMENATRIX SURVIVAL KIT – NORTH AFRICA PROTOCOL

PART 3: FIGHT BACK
(Localized Legal & Institutional Navigation)

THE DECISION MANUAL

This section is a decision manual. It assumes you have been targeted and are considering taking action.

THE GOLDEN RULE

Before you report to the police, you must assess if the law protects you or endangers you.

3.1 THE EVIDENCE VAULT (FORENSIC STANDARDS)

Stop. Do not report, block, or delete anything yet. Most legal cases fail because the evidence is "weak" (easily faked screenshots) or "gone" (deleted by the platform or the user). **What Counts as Valid Evidence?** Judges and police need proof that links a specific person to a specific crime at a specific time. A simple screenshot of a chat bubble is often rejected.

A) THE FORENSIC CHECKLIST

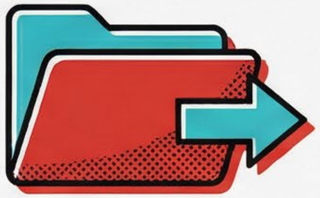
- **THE URL (The Address):** ⚠
  Why: Usernames (e.g., @RayenDiri) can be changed. The URL is often the only permanent link.
  How: On a browser, copy the full address (e.g., facebook.com/profile.php?id=1000….). On mobile, click 'Share Profile' > 'Copy Link'.

- **THE USER ID (The Fingerprint):** ⚠
  Why: Even if they change their URL, the Numeric User ID (e.g., 123456789) stays the same.
  How: Use free online tools (search 'Find Facebook ID') to reveal the permanent number behind the profile.

- **TIMESTAMPS:** ⚠
  Why: 'Yesterday' is not a date.
  How: Hover over the time (e.g., '2 hrs ago') on a desktop to see the exact date and time. Capture this in the screenshot.

- **THE CONTEXT (The Flow):** ⚠
  Why: Judges will ask, 'Did you provoke him?'
  How: Do not just screenshot the insult. Screenshot the messages before and after to prove you did not instigate the attack.

B) STORAGE PROTOCOL

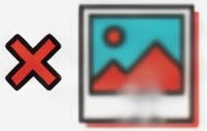


NAMING: Save files logically: YYYY-MM-DD_Platform_HarasserName_Content.jpg.

THE "VAULT": Store these files in a secure cloud (Google Drive/Dropbox) with 2FA enabled. Do not keep them only on your phone, which could be lost, broken, or confiscated.

C) EVIDENCE YOU THINK HELPS BUT DOESN'T

A simple screenshot of a chat bubble is often rejected.



Blurred or incomplete screenshots.

Evidence that has been deleted by the user or platform.

3.2 The Core: Tunisia Deep-Dive

Status: Strong laws on paper, dangerous application in practice.

1) The Legal Framework

Law 58 (2017):

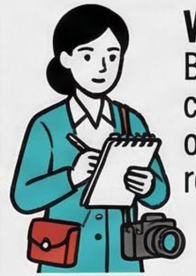
This is your shield.
Defines violence broadly.
Mandates police protection.

Decree 54 (2022):

Addresses cybercrime, but Article 24 penalizes "spreading false news."
Victims exposing harassers face counter-charges.

2) The Gold Standard Tool: Constat d'Huissier

In Tunisia, police dismiss screenshots.



What it is:
Bailiff views content, writes official legal report.

Why do it:
Makes evidence nearly impossible to contest in court.

Strategy:
Bailiff views or legal report.

Cost:

150 – 300 TND

Get this **BEFORE** you go to the police.

3) Reporting Pathways

A) Unités Spécialisées
(The Safe Door)

Specialized police for violence against women (Law 58). Better trained, privacy-focused. Call 1899.

B) The Public Prosecutor
(The Direct Door)

Filing directly at Tribunal of First Instance.
Bypasses police refusal.

C) Regular Police Station
(The Risky Door)

Officers often victim-blame, dismiss digital violence.
Avoid unless emergency.

4) Verified Support Contacts & Decision Map

ATFD
Legal counseling. +216 71 890 011 / ecoute@atfd-tunisie.org

Aswat Nissa
Political violence/smear campaigns. +216 55 809 834

Green Line 1899
Immediate government referral (24/7).

TUNISIA DECISION MAP

Political → Contact **Aswat Nissa** first. Do not go to police alone.

Domestic → Go to **Unités Spécialisées** using Law 58.

WOMENATRIX SURVIVAL KIT – NORTH AFRICA PROTOCOL

3.3 NORTH AFRICA FIELD GUIDE — COUNTRY RISK CARDS

MOROCCO

The Tool: E-Blagh (DGSN Portal)
- **Pros:** Digital, allows anonymity, handles sexual extortion effectively (20% of cases).
- **Cons:** State-monitored.

The Trap: Article 490 (Sex outside marriage)
- **Risk:** If you report sextortion (blackmail with nude images) and you are unmarried, you risk being charged with "debauchery".

The Protocol:
- If the threat involves intimate images, contact Union de l'Action Féminine (Annajda) (+212 537 700 964) before using E-Blagh to assess legal risk.
- **WARNING:** Do NOT use the "E-Police" app/portal. It requires ID verification. Only use E-Blagh for anonymous reporting.

EGYPT

The Pathway: Internet Investigation Directorate (Mabahith al-Internet)
- **Reality:** Requires physical reporting at Abbasiya (Cairo) or regional directorates. Online reporting is often insufficient.

The Trap: "Family Values" (Law 175, Art 25)
- **Risk:** Prosecutors may investigate you for the content of your images or posts if they violate "family principles," even if you are the victim.

The Protocol:
- Never report digital violence involving "contentious" material (dancing, liberal dress, intimacy) without a lawyer. Contact ECWR (+20 2 2528 2176) or NCW (15115) first.

LIBYA & SUDAN (Conflict Zones)

The Context: The state is often the predator. Police stations may be controlled by militias (Libya) or parties to the conflict (Sudan).

The Risk: Reporting to security forces can lead to arbitrary detention, sexual violence, or "honor" retaliation.

The Safer Entry Points:
- **Libya:** Use the 1417 Hotline (UNFPA/Ministry of Social Affairs). It is anonymous and confidential.
- **Sudan:** Rely on Emergency Response Rooms (ERRs) or SIHA Network (complaints@sihanet.org). Avoid SAF/RSF checkpoints with evidence on your phone.

MAURITANIA

The Risk: Zina Laws.
- **Reality:** Reporting sexual violence or sextortion can lead to prosecution for adultery if coercion cannot be strictly proved.

The Rule: NEVER go to the police alone.

The Protocol:
- You must be accompanied by an NGO like AMSME (Call 1013) to frame the complaint correctly and ensure you are treated as a victim.

WOMENATRIX SURVIVAL KIT – NORTH AFRICA PROTOCOL

3.4 Decision Tree: Should I Report?

Use this logic flow to decide your next move.

START HERE: Do you know who the harasser is?

NO (Anonymous / Fake Profile)

Is the threat immediate (death/kidnapping)?

- **YES:** Call emergency services (197 in Tunisia, 19 in Morocco).
- **NO: DO NOT REPORT.** Police investigations into anonymous accounts are slow and often dead ends. Focus on Blocking and Documentation (See 3.1).

YES (Known Individual)

Does the harassment involve "compromising" content (Intimate images/Chats)?

- **YES: STOP.** Check your country's laws (Art 490 Morocco / Art 25 Egypt / Zina Mauritania).
- **ACTION:** Contact an NGO (ATFD, UAF, ECWR) for a risk assessment before going to police.

NO (Threats, insults, defamation only):

Is the harasser state-linked (Police/Official)?

- **YES: HIGH RISK.** Reporting may lead to retaliation. Contact international human rights orgs (OMCT, Amnesty).
- **NO: SAFE TO REPORT.** Proceed to Specialized Units (Tunisia) or E-Blagh (Morocco).

THE STOP POINT: If the investigation requires you to hand over a phone containing "immoral" content in Egypt, Mauritania, or Morocco: **DO NOT FILE A POLICE REPORT.** The risk of arrest often outweighs the chance of justice. Use NGO support and technical blocking instead.

PART 4: HEAL THE HUMAN

(Psychological Survival — Regional Context)

This section is for women living with the aftermath. The attack happened. The immediate adrenaline is fading, and the pychological impact, shame, freeze, panic, is setting in. **This is not a therapy session.** These are **survival tools to stabilize your nervous system** so you can make decisions.

THE PSYCHOLOGICAL IMPACT: SHAME, FREEZE, PANIC.

SURVIVAL TOOLS: STABILIZE

4.1 GROUNDING TOOLKIT (IMMEDIATE STABILIZATION)

When panic hits, your brain disconnects. You might feel like you are floating, unable to speak, or stuck in a loop. Force your brain back into the "here and now."

THE 5-4-3-2-1 METHOD

Time: 60 seconds

1		**Name 5 things you can see.** (e.g., "I see a blue cup. I see a crack in the wall. I see my own hand.")
2		**Name 4 things you can touch.** (Touch them physically: the fabric of your chair, the cool table, your hair.)
3		**Name 3 things you can hear.** (Traffic outside, a fan humming, your own breath.)
4		**Name 2 things you can smell.** (Soap on your hands, coffee.)
5		**Name 1 thing you can taste.** (Or name a taste you like, like mint or lemon.)

THE CATEGORIES GAME

Time: 2 minutes

1. Pick a category. (e.g., Cities in Tunisia, types of fruit, colors, animals.)

2. List as many items in that category as possible in one minute.

3. Count them. Switch categories and repeat until your heart rate slows.

ANCHORING SCRIPTS

Use this when:

- You feel unsafe in your own home or body.

Say this out loud or repeat it silently until the words feel real.

"My name is **[Your Name].** I am safe in **[Current Room/Place].** This threat is digital, not physical right now. I am holding my phone; the phone is not holding me."

4.2 THE SUPPORT SQUAD MODEL (COLLECTIVE SURVIVAL)

Do not do this alone. Isolation feeds the trauma. The 'Support Squad' moves the burden from you (the survivor) to a trusted team. Assign these roles to friends or allies immediately.

ROLE 1: THE FILTERER

- **THE JOB:** They log into your accounts so you don't have to. They hide, mute, or delete abusive comments after they have been documented.
- **WHY:** Prevents the images/words from burning into your memory.
- **RULE:** They must never tell you the specific details of the hate unless it is a direct physical threat.

ROLE 2: THE DOCUMENTER

- **THE JOB:** They take the screenshots, capture the URLs, and save the evidence to a secure folder (The Vault).
- **WHY:** Legal evidence requires looking at the violence. You should not have to do that while traumatized.
- **RULE:** They must be meticulous (capturing dates/IDs) so it only needs to be done once.

ROLE 3: THE CAREGIVER

- **THE JOB:** They manage your physical reality. They remind you to drink water, eat, and sleep. They facilitate the grounding exercises.
- **WHY:** Trauma makes you forget basic biological needs.
- **RULE:** They do not talk about the online attack. They talk about real life (food, rest, comfort).

ROLE 4: THE REPORTER

- **THE JOB:** They deal with the platforms. They file the reports to Facebook, Instagram, or TikTok using the "Community Standards" forms.
- **WHY:** Reporting is frustrating and repetitive. It causes burnout.
- **RULE:** They keep a log of reference numbers for every report filed.

WOMENATRIX SURVIVAL KIT – NORTH AFRICA CONTACTS

VERIFIED SUPPORT CONTACTS

TUNISIA

ATFD
Type: Legal & Psychosocial Support (NGO)
Contact: +216 71 890 011 (Tunis Center) / ecoute@atfd-tunisie.org
Note: Can refer you to trusted lawyers.

Green Line
Type: Government Hotline (Ministry of Woman)
Contact: 1899 (Toll-free)
Note: Can direct you to "Unités Spécialisées" (Specialized Police Units).

Aswat Nissa
Type: Political/Digital Violence Support (NGO)
Contact: +216 55 809 834

Specialized & Regional Centers
Digital Citizenship Helpline: 56 563 501
Dr. Ahlam Belhadj Center (ATFD): 27 233 688 (Specialized Listening)
Jossour Al-Aman Center (Le Kef): 99 338 774
Centre Najia (Aswat Nissa): 54 542 500 (Sexual Violence Survivors)
Thiqar Center (Kasserine): 98 263 363

MOROCCO

Union de l'Action Féminine / Annajda Centers
Type: Legal Aid, Shelter, Counseling (NGO)
Contact: +212 537 700 964 (Rabat)
Note: Call here before going to police if unmarried.

E-Blagh Portal
Type: State Cybercrime Reporting
Contact: www.e-blagh.ma
Warning: State-monitored. Do not use if you are at risk of Article 490 (sex outside marriage).

ALGERIA

Réseau Wassila
Type: Network of organizations for women victims of violence (NGO)
Contact: 0560 100 105.
Note: Operating hours are Sun–Thu, 9:00 AM – 4:30 PM. If you call outside these hours, leave a message or email ecouteresauwassila@gmail.com.

EGYPT

National Council for Women (NCW)
Type: State Body / Ombudsman
Contact: 15115 (Hotline)
Note: Can help navigate the legal system.
SAFETY TIP: If your abuser checks your phone, delete this call from your history immediately after hanging up.

Egyptian Center for Women's Rights (ECWR)
Type: Legal Advocacy (NGO)
Contact: +20 2 2528 2176 ("Ask Nehad" Campaign)
Warning: Do not report "morality" related cases to police without a lawyer.

LIBYA

1417 Hotline
Type: Psychosocial Support (UNFPA / Ministry of Social Affairs)
Contact: 1417
Note: Anonymous and confidential.
SAFETY TIP: If your abuser checks your phone, delete this call from your history immediately after hanging up.
Safety Warning: Avoid reporting to militias or local security forces. Risk of arbitrary detention is high.

MAURITANIA

AMSME (Association Mauritanienne pour la Santé de la Mère et de l'Enfant)
Type: Emergency GBV Support (NGO)
Contact: 1013 (Green Number)
Safety Warning: NEVER go to the police alone. You must be accompanied by an NGO to avoid Zina (adultery) counter-charges.

SUDAN

SIHA Network
Type: Documentation & Support (NGO)
Contact: complaints@sihanet.org / Signal
(Use verified local contacts).

Emergency Response Rooms (ERRs)
Type: Community-based mutual aid
Contact: Search "Khartoum State ERR" or "Emergency Response Room" on Facebook/Twitter to find your local number. Immediately switch to Signal for the actual conversation.
Safety Warning: Do not cross checkpoints with evidence of reporting on your phone.

CONCLUSION: RECLAIMING YOUR SPACE

Survival is Not the End Goal. Freedom Is.

The New Normal: Digital Resilience

- **Keep the Fortress Built:** Maintain your 2FA, keep your passwords strong, and regularly audit your privacy settings.
- **Stay Connected:** Do not retreat into isolation. Your "Support Squad" is your strongest defense against future attacks.
- **Share the Knowledge:** If you see another woman being targeted, share this guide. We are safer when we all know how to fight back.

A Final Note on Justice

Justice in our region is often flawed, slow, or even hostile. If the legal system fails you, remember that survival is its own form of justice. Denying your abuser the power to destroy your life is a victory.

You are the glitch in their system. Stay loud. Stay safe.

Womenatrix Survival Kit

While laws and algorithms evolve, the strategies outlined here represent a verified snapshot of digital safety mechanisms in North Africa as of December 2025. To ensure this knowledge remains accessible, we have released this guide as an Open Source Resource. We encourage activists, researchers, and legal experts to adapt, translate, and build upon this framework for their own communities.