



E-RADAR · الرادار

A practical guide

Digital Safety & Security Guide

For women, girls and LGBTQI+ people facing gender-based digital violence in Tunisia — and for anyone who supports them.

Secure your accounts and phone

What to do if it happens

Evidence log & safety plan

Where to get help

In danger right now?

1899 free helpline for women victims of violence · **197** police · **193** national guard · **190** SAMU

Contents

1	How to use this guide	3
2	Understanding gender-based digital violence	4
3	Secure your accounts	6
4	Your phone and devices	8
5	Privacy settings, platform by platform	10
6	If it happens: response sheets	12
7	Documenting and preserving evidence	15
8	My personal safety plan	17
9	Legal basics in Tunisia	18
10	Looking after yourself	19
11	Where to get help	20
12	One-page checklists	21

How to use this guide

This guide is for you if someone is using the internet, a phone or an app to hurt you, scare you, control you or silence you — or if you simply want to be better protected. It is also for friends, family and professionals who want to help.

Read only what you need

Every chapter stands on its own. If something is happening right now, go straight to chapter 6, “If it happens”.

You decide

You don’t have to report anything, to anyone. Using this guide does not commit you to any step. Every decision stays yours.

Go at your own pace

Some parts can be hard to read. Take breaks. You can ask someone you trust to read with you.

What you will find

- **Understand** what gender-based digital violence is (chapter 2).
- **Protect** your accounts, your phone and your privacy (chapters 3 to 5).
- **Act** if something happens, with short response sheets (chapter 6).
- **Document** what happens and **plan** your safety, with worksheets to fill on paper (chapters 7 and 8).
- **Know** your rights, look after yourself and find help (chapters 9 to 11).
- **Check** yourself with one-page checklists (chapter 12).



Is someone watching your screen or phone?

If you think someone checks your phone or computer, read this guide on a device they cannot access (a trusted friend’s phone, a work or library computer), or keep the printed copy somewhere safe.

On the E-RADAR website, the “**Quick exit**” button at the top of every page — or pressing **Esc twice** — takes you instantly to Google. Afterwards, you can also delete the site from your browser history, or use a private / incognito window.



If you are in immediate danger

Call **197** (police), **193** (national guard) or **190** (SAMU, medical emergency). The free helpline for women victims of violence is **1899**.

A note on words: we say “you” throughout. This guide is for all women and girls, and for all LGBTQI+ people, whatever their identity. Menu names in apps change often: if a setting has a slightly different name on your phone, use the search bar inside the app’s settings.

Understanding gender-based digital violence

Gender-based digital violence is any act carried out through the internet, phones or apps that aims to harm, frighten, silence or control someone because she is a woman or a girl, or because of their gender identity or sexual orientation.

It is real violence. Its effects on your mental health, your safety, your studies, your work and your relationships are real. It often comes from someone close: a partner or ex-partner, a family member, a colleague, a classmate. It can also come from strangers, sometimes organised in groups.

Why “gender-based”?

Women and LGBTQI+ people are targeted in specific ways: comments about their bodies, threats to share intimate images, being outed to their family, reputation attacks. Social and family pressure can make the consequences much heavier — and make it harder to talk about it.

Common forms

Form	What it looks like
Harassment	Repeated insulting, sexual or unwanted messages and comments, often from several accounts.
Threats	Messages threatening violence, exposure, or harm to you or people close to you.
Blackmail	“Do this, or I will publish / tell...” — demands for money, images, a meeting, or silence.
Sextortion	Blackmail using intimate images or videos, real or fake.
Non-consensual intimate images	Sharing, or threatening to share, intimate images without consent — including images taken secretly and deepfakes (fake images made with AI using your face).
Defamation	Spreading lies or rumours to damage your reputation.
Cyberstalking	Monitoring, following or tracking you online or through your phone: constant messages, location tracking, spyware.
Hate speech	Attacks targeting you because you are a woman or LGBTQI+, sometimes calling for violence.
Outing	Revealing — or threatening to reveal — someone’s sexual orientation or gender identity without consent.
Impersonation	Fake accounts using your name or photos, or someone taking over your account to speak as you.
Doxxing	Publishing your personal information: address, phone number, workplace, family details.

Warning signs

Digital violence sometimes starts with small things. These signs can help you name what is happening:

- You feel afraid or anxious every time you receive a message from a certain person.
- Someone asks for your passwords, checks your phone, or wants to know where you are all the time.
- Someone knows things you never told them: where you were, who you met, what you wrote.
- Someone threatens to share images, conversations or information about you.
- Someone asks for money or images in exchange for not publishing something.
- You find an account using your name or your photos that you did not create.
- You receive insulting comments about your body, your identity or your orientation.

If one of these sounds like your situation, you have the right to ask for support. You don't need to wait until it gets worse.

It is not your fault. Not because you trusted someone, not because you shared a photo, not because of what you wear, say or post, not because of who you are or who you love. The responsibility lies entirely with the person who harms you.

Secure your accounts

Most account takeovers rely on a weak or reused password, a stolen code, or someone close who knows your phone. A few changes make a big difference.



If someone close may be watching your accounts

Make changes from a safe device they cannot access. Suddenly locking someone out can alert them — if that could put you at risk, first think through your safety plan (chapter 8) or ask for support.

1. Start with your email

Your email is the master key: whoever controls it can reset the passwords of all your other accounts. Secure it first, then your phone number's accounts, then social media.

2. Strong, different passwords

- Use a **passphrase**: four or more random words, easy for you to remember, hard to guess. For example: **olive-bus-cloud-river-27** (don't use this one!).
- **Never reuse** the same password on two accounts. When one site leaks, attackers try that password everywhere.
- Avoid birthdays, names, pets, phone numbers — people close to you can guess them.
- A **password manager** (an app that remembers all your passwords in an encrypted vault, such as Bitwarden, or the one built into your phone or browser) makes this easy. You only remember one strong passphrase.
- Do not share your passwords with a partner, even “as proof of trust”. Asking for them can be a form of control.

3. Turn on two-factor authentication (2FA)

With 2FA, logging in from a new device needs a second code in addition to your password. Even if someone knows your password, they cannot get in.

- **Best:** an authenticator app (Google Authenticator, Microsoft Authenticator, Aegis...) or a passkey.
- **OK:** codes by SMS — better than nothing, but weaker, especially if someone can access your SIM card or phone.

Platform	Where to find it
Facebook & Instagram	Settings → Accounts Center → Password and security → Two-factor authentication → choose the account → Authentication app (recommended).
WhatsApp	Settings → Account → Two-step verification → Turn on → choose a 6-digit PIN nobody knows → add an email address so you can reset it.
Google / Gmail	Google Account (myaccount.google.com) → Security → 2-Step Verification → follow the steps; add an authenticator app and backup codes.

Platform	Where to find it
TikTok	Profile → ☰ menu → Settings and privacy → Security → 2-step verification .

4. Keep your recovery codes safe

When you turn on 2FA, the platform gives you **recovery (backup) codes**. They let you get back into your account if you lose your phone. Write them down or print them and keep them somewhere safe that the person harming you cannot reach. Never send a code to anyone — not even someone claiming to be “support”.

5. Check who is logged in

Look regularly at active sessions and devices, and log out of anything you don’t recognise:

- **Facebook / Instagram:** Accounts Center → Password and security → **Where you’re logged in**.
- **WhatsApp:** Settings → **Linked devices**. A linked computer can read all your messages.
- **Google:** Google Account → Security → **Your devices**. The **Security Checkup** walks you through everything.
- **TikTok:** Settings and privacy → Security → **Manage devices**.

Also check the recovery email and phone number on each account, and the third-party apps connected to it. Remove anything that is not yours.

6. Watch out for links and fake “support”

Never enter your password on a page you reached through a link in a message, even if it looks official. Open the app or type the address yourself. Platforms never ask for your code or password by message.



Tip

Do one account per day: email first, then WhatsApp, then Facebook/Instagram, then the rest. Small steps are still steps.

Your phone and devices

Your phone holds your messages, photos, location and accounts. Whoever has physical access to it, even for a few minutes, can do a lot. Here is how to protect it.

Screen lock

- Use a PIN of at least 6 digits or a passcode. Avoid simple patterns and dates.
- Be careful with fingerprint or face unlock if someone could force you or use it while you sleep.
- Don't share your code. If someone already knows it, change it.
- Hide notification content on the lock screen, so messages and codes cannot be read without unlocking.

Apps you don't recognise

Go through the full list of apps (Settings → Apps). Some spy apps hide behind ordinary names like "System service" or "Sync". Also check:

- **Android:** Settings → Security → **Device admin apps**, and apps with access to Accessibility, notifications or location. Make sure **Google Play Protect** is on.
- **iPhone:** Settings → General → **VPN & Device Management** (unknown profiles). **Safety Check** (Settings → Privacy & Security) shows who you share access with and lets you stop it.

Signs of stalkerware (spy apps)

- Someone knows your messages, conversations or movements without you telling them.
- The battery drains unusually fast, or the phone heats up when you are not using it.
- Mobile data use jumps for no reason.
- Settings changed without you (location on, security settings off).
- The person had your phone in their hands, or "set it up" for you.



Don't delete a spy app right away

If you suspect stalkerware, removing it can alert the person and make the situation more dangerous. It also removes evidence. First make a safety plan (chapter 8), use another device to ask for help, and get technical support. When it is safe, a full factory reset — after saving your evidence — is the most reliable cleanup.

Location sharing

- Check whether you share your location in **Google Maps** (Location sharing), **Find My** on iPhone (Share My Location), **Snapchat** (Snap Map — use Ghost Mode), and family-tracking apps.
- Turn off location for apps that don't need it (Settings → Location / Privacy → Location Services).
- Avoid posting your location in real time. Post after you have left a place.

Physical trackers

Small Bluetooth trackers (AirTag type) can be hidden in a bag, a coat or a car.

- **iPhone** warns you when an unknown tracker moves with you ("AirTag Found Moving With You").

- **Android** has **Unknown tracker alerts** (Settings → Safety & emergency) and a manual scan.
- If you find one, think about your safety before removing it: the person may notice. Photograph it, note where and when you found it, and ask for support.

Photos reveal more than you think

Photos can contain hidden information (metadata): the exact place and time they were taken. Turn off location tagging in your camera settings. When sharing on iPhone, tap **Options** and turn off **Location**; in Google Photos, use **Remove location**. Also check backgrounds: a street sign, a school uniform or a window view can reveal where you are.

Backups and cloud

Your photos and messages are often copied to **iCloud**, **Google Photos / Google Drive** or a WhatsApp backup. Anyone who knows that account's password can see everything, from any device. Secure those accounts as described in chapter 3, and check which devices are signed in to them.

Updates

Install system and app updates regularly. They fix security holes that attackers use.



Shared or second-hand phone?

If a phone was given to you, or someone else set it up, they may still have access to its accounts. Sign in with your own new email account, and check “Linked devices” and signed-in devices everywhere.

Privacy settings, platform by platform

Privacy settings decide who can see you, contact you and find you. Ten minutes per platform is enough.

Menu names change between app versions and languages. If you can't find a setting, type its name into the search bar inside the app's settings.

Facebook

- ☐ Run **Privacy Checkup** (Settings & privacy) — it walks you step by step.
- ☐ Set future posts to **Friends**, not Public. Use **Limit past posts** for old ones.
- ☐ Hide your friends list, phone number, email and date of birth.
- ☐ Turn on **Tag review** and **Profile review**, so nothing appears on your profile without your approval.
- ☐ Limit who can send you friend requests and who can look you up by phone number or email.
- ☐ Use **Block** for abusive accounts, and **Restrict** if you don't want them to know.

Instagram

- ☐ Switch to a **Private account**.
- ☐ Use **Restrict** (they won't know) or **Block** for problem accounts — including new accounts they may create.
- ☐ Choose who can message you, comment, tag and mention you.
- ☐ Turn on **Hidden Words** to filter offensive comments and message requests.
- ☐ Use **Limits** to temporarily hide comments and messages from accounts that don't follow you or followed you recently — useful during an attack.
- ☐ Use **Close Friends** for personal stories, and hide your activity status.

WhatsApp

- ☐ Settings → Privacy: choose who sees your **Last seen & online**, **Profile photo**, **About** and **Status**.
- ☐ **Groups**: “My contacts” only, so strangers can’t add you.
- ☐ **Calls** → **Silence unknown callers**.
- ☐ Check **Linked devices** regularly.
- ☐ The **Privacy checkup** (Settings → Privacy) groups all of this in one place.
- ☐ Remember: disappearing messages and “view once” don’t stop someone from photographing the screen.

TikTok

- ☐ Switch to a **Private account**.
- ☐ Turn off **Suggest your account to others** (including to contacts and Facebook friends).
- ☐ Choose who can comment, **Duet**, **Stitch**, download your videos and send you messages.
- ☐ Use comment **filters** and keyword filters.
- ☐ Hide your activity status and who you follow.



Do a “search yourself” check

Search your name, your username and your phone number in a search engine and on each platform, logged out or from a friend’s device. You will see what strangers see.

If it happens: response sheets

Short, practical sheets for the most common situations. Read the one you need. In every case: it is not your fault, you can document before blocking, and you can ask for support at any step.

6.1 My account was hacked

Signs: messages you didn't send, a changed password, you can't log in.

- 1 **Try to recover it** with the official tools: Facebook facebook.com/hacked · Instagram instagram.com/hacked · Google/Gmail g.co/recover · WhatsApp: register your number again on your phone, which logs the other person out, then turn on two-step verification.
- 2 **Once back in:** set a new strong password, change your email password too, log out of all unknown sessions, turn on 2FA, check the recovery email/phone and connected apps.
- 3 **Warn your contacts** not to answer messages asking for money, photos or codes.
- 4 **Document:** screenshots of messages sent in your name and of changes to the account.

If the person who got in is close to you and has access to your phone, do all of this from another, safe device.

6.2 I'm being threatened

- 1 **Assess the risk.** Does the person know where you live, work or study? Do the threats mention physical harm? Are they getting more frequent? If yes to any of these, take it seriously: call **1899**, or the police **197** if the danger is close.
- 2 **Don't answer or provoke.** Replying can escalate things.
- 3 **Document everything** (chapter 7) — keep the original messages even after blocking.
- 4 **Block and report** to the platform once you have saved the evidence.
- 5 **Plan your safety:** tell someone you trust, vary your routes and times if the person knows them, turn off location sharing.

6.3 I'm being blackmailed or sextorted

What happened is not your fault. The responsibility lies entirely with the person who is blackmailing you.

- 1 **Don't pay and don't send more images.** Paying rarely stops blackmail; it often leads to more demands.
- 2 **Don't delete the conversation.** Take screenshots showing the account name, its link and the date.
- 3 **Stop the contact** after documenting. Don't negotiate. You can deactivate your account temporarily instead of deleting it.

- 4 **Secure your accounts:** change passwords, turn on 2FA, make profiles private, hide friends and followers lists.
- 5 **Report the account** to the platform — they have dedicated procedures for intimate images.
- 6 **Protect your images** with StopNCII.org or Take It Down (see 6.4).
- 7 **Talk to someone** you trust, and ask for support.

6.4 My intimate images were shared (or may be)

Whether you sent an image in trust, were filmed without knowing, or a fake was made with AI — in every case, it is not your fault.

- 1 **Document where it appears** (link, account, date) without sharing it again.
- 2 **Report to the platform** using the option for intimate images shared without consent. Platforms prioritise these reports.
- 3 **StopNCII.org** (if you were 18 or older in the image): creates a digital “fingerprint” (hash) of your images on your own device — the image itself is never uploaded — so partner platforms can block it.
- 4 **Take It Down** (takeitdown.ncmec.org): the same approach if you were under 18 in the image.
- 5 **Search engines:** Google offers an official request form to remove non-consensual intimate images from its search results.
- 6 **Ask for support**, psychological and legal. You are not alone.



Never send the images

Don't send intimate images to anyone to “prove” what happened — not to us, not to anyone. A description and the link to the post are enough.

6.5 Being outed, or threatened with outing

Your identity belongs to you. Only you decide who knows, and when.

In Tunisia, being outed can lead to family rejection, losing housing or work, physical violence, or legal problems. We treat this situation as potentially dangerous.

If someone threatens to out you

- 1 **Don't pay or send anything.** This is blackmail; paying doesn't stop it.
- 2 **Document** the threat and keep the evidence somewhere safe — not on a shared phone.
- 3 **Reduce what can be found about you:** clean up your accounts, hide friends lists, remove photos that could be used, and check other accounts (dating apps, old profiles, group chats).
- 4 **Make a safety plan:** where could you go if things get difficult at home? Who could you call? What would you take? (chapter 8)
- 5 **Ask for support** from people and organisations that respect LGBTQI+ people. E-RADAR can help you find them.

If you have been outed

- Your physical safety comes first. If you are in danger, call **197** or **193**, or go to a safe person or place.
- Report the posts: revealing someone's orientation or identity is against the rules of most platforms.
- Psychological support matters a lot right now. You are not alone.

Before considering going to the authorities, get legal support to understand the risks and your options.

6.6 An online hate campaign against me

Insults or mockery about your gender, body, identity or orientation; calls for violence; many accounts attacking at once to silence you.

- 1 **Don't read everything yourself.** Ask someone you trust to sort and document for you.
- 2 **Document** posts and accounts, especially those with threats, incitement or your personal information.
- 3 **Use platform tools:** keyword filters, limit comments, Restrict or Block, Instagram "Limits".
- 4 **Report:** platforms ban hate speech based on gender, identity and orientation.
- 5 **Take a break:** make your account private or deactivate it temporarily until things calm down.

If the attack includes threats or your address, also follow sheet 6.2.

Hate says something about the person who writes it, not about you.

6.7 I'm being stalked online

Signs: repeated messages or calls after you said stop; new accounts every time you block; they know where you were or who you were with; gifts or messages arriving where you go.

How they may know where you are: location sharing in an app, stalkerware on your phone, a physical tracker in your belongings or car, or location details in your posts or your friends' posts.

- 1 **Document each incident** in your log (chapter 7): date, time, what happened.
- 2 **Check and turn off location sharing** (chapter 4).
- 3 **If you suspect a spy app, don't remove it straight away** — the person may notice. Ask for technical support first.
- 4 **Tell someone you trust** and make a safety plan.



Stalking can become physical danger

If you feel in danger, call **197** (police), **193** (national guard) or **1899**.

Documenting and preserving evidence

Documenting doesn't commit you to anything. But if one day you want to report or file a complaint, the evidence will be there.

What to save

- ☐ Screenshots of messages, comments or posts, **showing the date and time**.
- ☐ The **account name and its link** (profile URL or @username) — not only the display name, which can change.
- ☐ Links to posts, videos or pages.
- ☐ Call logs and SMS.
- ☐ Emails, with sender address.
- ☐ A short summary: what happened, when, where, who saw it.

How to take good screenshots

- Make sure the screenshot shows the account name, the date/time and the full message.
- For a profile, capture the page with its URL visible (on a computer, the address bar).
- For a long conversation, take several overlapping screenshots, in order.
- On WhatsApp, you can also **export the chat** (Chat → More → Export chat) — keep the export file.
- Some platforms let you **download your data** (Facebook, Instagram, Google Takeout), which includes messages.

How to keep evidence safe

- Store it where the person harming you can't reach it — not on a shared phone or shared cloud account.
- Keep a **second copy** in another safe place (a USB key, a separate email account only you know, a trusted person).
- Don't edit, crop or annotate the original files. Make copies if you need to.
- Give files clear names: **2026-03-14_instagram_@account_threat.png**.



Documenting can be painful

Looking at abusive content again is hard. You can ask someone you trust to do it with you or for you. Take breaks.



Intimate images

Don't send intimate images to anyone as evidence. Write down the link and a description; professionals will tell you how to proceed safely.

Incident log

Fill in one line per incident. Keep this sheet in a safe place. Make as many copies as you need.

Date	Time	Platform	Account / link	What happened	Screenshot saved where?	Witnesses

Example: 14/03 · 22:10 · Instagram · @example_account (instagram.com/example_account) · Threatened to send my photos to my brother · USB key, folder “March” · My friend S. saw the message.

My personal safety plan

A safety plan is a set of decisions you make calmly, in advance, so you know what to do if things get worse. Fill it in on paper, alone or with someone you trust. Keep it hidden, or keep it in your head.



Keep this plan safe

If the person harming you lives with you or checks your things, don't leave this page where they could find it. You can give a copy to a trusted person.

People I trust

who I can call or go to, any time

Safe places

where I can go if I need to leave quickly

Code word

a word or emoji that tells my trusted people "I need help, call / come now"

Safe device

a phone or computer the person can't access

Safe accounts

an email account only I know, for help and evidence

Where my evidence is stored

and who has a second copy

Things I would take

if I had to leave

☐ ID card / passport · ☐ phone and charger · ☐ money / bank card ·
☐ keys · ☐ medicines · ☐ important documents · ☐ this plan and my
 recovery codes · ☐ something that comforts me

Emergency numbers

1899 free helpline for women victims of violence · **197** police · **193**
 national guard · **190** SAMU

Legal basics in Tunisia

This chapter gives general information to help you understand your rights. It is not legal advice and does not replace a consultation with a lawyer or a qualified legal professional.

Organic Law no. 2017-58 on the elimination of violence against women

This law recognises several forms of violence against women — physical, moral (psychological), sexual, economic and political. It gives victims rights to protection, information and guidance, and to legal and psychological support.

Organic Law no. 2004-63 on the protection of personal data

This law protects your personal data. Publishing your information or images without your consent may be against the law.

Where you can turn

- The free helpline **1899** for women victims of violence.
- The specialised units for investigating violence against women within the police and the national guard.
- Associations that offer free legal support and accompaniment.

Before you decide

- Document first (chapter 7): good evidence helps in any procedure.
- You can be accompanied by a trusted person or a legal professional.
- Ask what will happen next, who will be informed, and how your information will be protected.



An honest note

We know that some people — especially LGBTQI+ people — may be afraid to go to the authorities, and that this fear can be well founded. Going to the police or to court is always your choice. Legal support can help you understand the risks and the options before you decide, and some steps (documenting, reporting to platforms, protecting your images) don't require any official procedure.

Disclaimer: the information in this chapter is general and may change. It is not legal advice. For your situation, consult a lawyer or a legal support service. Intersection Association cannot be held responsible for decisions taken solely on the basis of this guide.

Looking after yourself

Digital violence doesn't stay on the screen. It affects sleep, mood, concentration and relationships. Taking care of yourself is part of protecting yourself.

Normal reactions

After digital violence, many people feel: fear every time the phone buzzes, shame or self-blame, anxiety, difficulty sleeping, wanting to withdraw, or anger. Some feel numb. These are normal reactions to a situation that is not normal.

Small things that help

Less screen

Limit the time spent reading comments or messages. Let someone you trust check them for you.

Fewer alerts

Turn off notifications from the apps that stress you, or mute certain words and accounts.

A simple routine

Sleep, meals, a little movement. Small regular things give back a sense of control.

Someone to talk to

Talk to a person you trust. You don't have to tell everything.

Think about what makes you feel safe: a place, a person, an activity, music. Write it down on your safety plan.

What psychological support looks like

- A trained person listens without judging you.
- You choose what to talk about, at your own pace.
- They help you understand what you feel and find ways to cope with stress.
- Everything is confidential, with your consent.

You can ask for psychological support through E-RADAR: e-radar.intersection.uno/en/support/

If you are supporting someone

- Believe them. Say: "It's not your fault."
- Listen more than you advise. Let them decide.
- Don't share their story or images, even to "help".
- Offer practical help: documenting, sitting with them while they report, finding information.
- Look after yourself too.



If you are thinking of hurting yourself

Please talk to someone now: a person you trust, or call SAMU on **190**. You deserve help and support.

Where to get help

You are not alone. Here is who you can contact.

1899

Free helpline for women victims of violence

197

Police

193

National guard

190

SAMU — medical emergency

E-RADAR — e-radar.intersection.uno

A confidential platform by Intersection Association, in Darja, French and English.

Report an incident	Describe what happened, anonymously if you wish. /en/report/
Ask for help	Psychological, legal or technical support. /en/support/
Track with your code	After sending, you get a follow-up code. Keep it safe: it lets you follow your report without giving your name. /en/track/
In danger now?	What to do right away. /en/danger/
Resources	Short guides on each topic in this guide. /en/resources/

Lost your follow-up code? It can't be recovered, but you can always send a new report or request.

Platform help pages

- Hacked accounts: facebook.com/hacked · instagram.com/hacked · g.co/recover
- Intimate images: StopNCII.org · takeitdown.ncmec.org

Trusted organisations near me

To be filled in by Intersection or by you: organisations, services and people you can turn to locally.

Name	What they offer	Contact

One-page checklists

Tick as you go. You don't have to do everything at once.

Account security

- ☐ My email has a strong, unique passphrase and 2FA.
- ☐ Every important account has its own password (or I use a password manager).
- ☐ 2FA is on: Facebook/Instagram, WhatsApp (PIN), Google, TikTok.
- ☐ My recovery codes are written down and stored safely.
- ☐ I checked active sessions and logged out unknown devices.
- ☐ Recovery email and phone number are mine and up to date.
- ☐ I removed connected apps I don't use.
- ☐ Nobody else knows my passwords or codes.

My phone

- ☐ Screen lock with a 6+ digit PIN that nobody knows.
- ☐ Notification content hidden on the lock screen.
- ☐ I reviewed my apps and their permissions (location, microphone, accessibility).
- ☐ Location sharing is off where I don't need it (Maps, Find My, Snap Map).
- ☐ Camera location tagging is off.
- ☐ My cloud account (iCloud / Google) is secured and I know which devices are signed in.
- ☐ WhatsApp "Linked devices" checked.
- ☐ System and apps are up to date.

If I'm being blackmailed

- ☐ I don't pay and I don't send anything else.
- ☐ I don't delete the conversation.
- ☐ I took screenshots with the account name, link and date.
- ☐ I stopped responding after documenting.
- ☐ I changed my passwords and turned on 2FA.
- ☐ I made my accounts private and hid my friends/followers lists.
- ☐ I reported the account to the platform.
- ☐ I used StopNCII.org / Take It Down if images are involved.
- ☐ I told someone I trust.
- ☐ I know the numbers: **1899 · 197 · 193 · 190**.

It is not your fault. You are not alone.



**You are not alone. We are with
you.**

E-RADAR is a confidential platform by Intersection Association for women, girls
and LGBTQI+ people facing gender-based digital violence in Tunisia.

e-radar.intersection.uno

1899 · 197 · 193 · 190

This guide gives general information. It is not legal, medical or technical advice for your
specific situation. Menu names in apps change over time. 2026 edition.