



E-RADAR · الرادار

Un guide pratique

Guide de sécurité numérique

Pour les femmes, les filles et les personnes LGBTQI+ confrontées aux violences numériques fondées sur le genre en Tunisie — et pour toutes les personnes qui les soutiennent.

Protéger vos comptes et votre téléphone

Que faire si cela arrive

Journal des preuves & plan de sécurité

Où trouver de l'aide

En danger maintenant ?

1899 numéro vert pour les femmes victimes de violence · **197** police · **193** garde nationale · **190** SAMU

Sommaire

1	Comment utiliser ce guide	3
2	Comprendre les violences numériques fondées sur le genre	4
3	Protéger vos comptes	6
4	Votre téléphone et vos appareils	8
5	Les paramètres de confidentialité, plateforme par plateforme	10
6	Si cela arrive : fiches réflexes	12
7	Garder et conserver les preuves	16
8	Mon plan de sécurité personnel	18
9	Repères juridiques en Tunisie	19
10	Prendre soin de vous	20
11	Où trouver de l'aide	21
12	Listes de vérification d'une page	23

Comment utiliser ce guide

Ce guide est pour vous si quelqu'un utilise internet, un téléphone ou une application pour vous faire du mal, vous faire peur, vous contrôler ou vous faire taire. Ou si vous voulez simplement mieux vous protéger. Il s'adresse aussi aux proches et aux professionnel·les qui veulent aider.

Lisez seulement ce dont vous avez besoin

Chaque chapitre se lit seul. Si quelque chose se passe en ce moment, allez directement au chapitre 6, « Si cela arrive ».

C'est vous qui décidez

Vous n'êtes obligé·e de signaler quoi que ce soit à personne. Lire ce guide ne vous engage à rien. Chaque décision vous appartient.

Allez à votre rythme

Certaines parties peuvent être difficiles à lire. Faites des pauses. Vous pouvez demander à une personne de confiance de lire avec vous.

Ce que vous trouverez

- **Comprendre** ce que sont les violences numériques fondées sur le genre (chapitre 2).
- **Protéger** vos comptes, votre téléphone et votre vie privée (chapitres 3 à 5).
- **Agir** si quelque chose arrive, grâce à des fiches réflexes courtes (chapitre 6).
- **Garder une trace** de ce qui se passe et **préparer** votre sécurité, avec des fiches à remplir sur papier (chapitres 7 et 8).
- **Connaître** vos droits, prendre soin de vous et trouver de l'aide (chapitres 9 à 11).
- **Faire le point** avec des listes de vérification d'une page (chapitre 12).



Quelqu'un surveille votre écran ou votre téléphone ?

Si vous pensez que quelqu'un consulte votre téléphone ou votre ordinateur, lisez ce guide sur un appareil auquel cette personne n'a pas accès (le téléphone d'une amie de confiance, un ordinateur au travail ou à la bibliothèque), ou gardez la version imprimée dans un endroit sûr.

Sur le site E-RADAR, le bouton « **Sortie rapide** » en haut de chaque page — ou **appuyer deux fois sur Échap** — vous envoie immédiatement sur Google. Vous pouvez aussi effacer ensuite le site de votre historique, ou utiliser une fenêtre de navigation privée.



Si vous êtes en danger immédiat

Appelez le **197** (police), le **193** (garde nationale) ou le **190** (SAMU, urgence médicale). Le numéro vert pour les femmes victimes de violence est le **1899**.

Un mot sur le langage : nous vous disons « vous » tout au long du guide et nous utilisons l'écriture inclusive. Ce guide s'adresse à toutes les femmes et à toutes les filles, et à toutes les personnes LGBTQI+, quelle que soit leur identité. Les noms des menus changent souvent dans les applications : si un réglage porte un nom un peu différent sur votre téléphone, utilisez la barre de recherche dans les paramètres de l'application.

Comprendre les violences numériques fondées sur le genre

Une violence numérique fondée sur le genre, c'est tout acte commis par internet, par téléphone ou via une application pour nuire à une personne, lui faire peur, la faire taire ou la contrôler parce qu'elle est une femme ou une fille, ou en raison de son identité de genre ou de son orientation sexuelle.

C'est une vraie violence. Ses effets sur votre santé mentale, votre sécurité, vos études, votre travail et vos relations sont bien réels. Elle vient souvent d'une personne proche : un·e partenaire ou ex-partenaire, un membre de la famille, un·e collègue, un·e camarade de classe. Elle peut aussi venir d'inconnu·es, parfois organisé·es en groupe.

Pourquoi « fondée sur le genre » ?

Les femmes et les personnes LGBTQI+ sont visées de façon spécifique : commentaires sur leur corps, menaces de diffuser des images intimes, révélation de leur orientation ou identité à leur famille, atteintes à leur réputation. La pression sociale et familiale peut rendre les conséquences bien plus lourdes — et rendre encore plus difficile d'en parler.

Les formes les plus courantes

Forme	À quoi cela ressemble
Harcèlement	Messages et commentaires insultants, sexuels ou non désirés, répétés, souvent depuis plusieurs comptes.
Menaces	Messages qui menacent de violence, de divulgation, ou de faire du mal à vous ou à vos proches.
Chantage	« Fais ça, sinon je publie / je raconte... » — exigences d'argent, d'images, d'un rendez-vous ou de silence.
Sextorsion	Chantage à partir d'images ou de vidéos intimes, réelles ou fausses.
Images intimes diffusées sans consentement	Partager, ou menacer de partager, des images intimes sans consentement — y compris des images prises en cachette et des deepfakes (fausses images fabriquées par IA avec votre visage).
Diffamation	Répandre des mensonges ou des rumeurs pour nuire à votre réputation.
Cyberharcèlement obsessionnel (cyberstalking)	Vous surveiller, vous suivre ou vous pister en ligne ou via votre téléphone : messages incessants, suivi de votre localisation, logiciels espions.
Discours de haine	Attaques qui vous visent parce que vous êtes une femme ou une personne LGBTQI+, parfois avec des appels à la violence.
Outing	Révéler — ou menacer de révéler — l'orientation sexuelle ou l'identité de genre de quelqu'un sans son consentement.

Forme	À quoi cela ressemble
Usurpation d'identité	Faux comptes avec votre nom ou vos photos, ou quelqu'un qui prend le contrôle de votre compte pour parler à votre place.
Doxxing	Publication de vos informations personnelles : adresse, numéro de téléphone, lieu de travail, détails sur votre famille.

Les signaux d'alerte

La violence numérique commence parfois par de petites choses. Ces signes peuvent vous aider à mettre des mots sur ce qui se passe :

- Vous avez peur ou vous êtes angoissé-e à chaque message d'une certaine personne.
- Quelqu'un vous demande vos mots de passe, fouille votre téléphone ou veut savoir où vous êtes en permanence.
- Quelqu'un sait des choses que vous ne lui avez jamais dites : où vous étiez, qui vous avez vu, ce que vous avez écrit.
- Quelqu'un menace de diffuser des images, des conversations ou des informations sur vous.
- Quelqu'un vous demande de l'argent ou des images en échange de ne pas publier quelque chose.
- Vous trouvez un compte avec votre nom ou vos photos que vous n'avez pas créé.
- Vous recevez des commentaires insultants sur votre corps, votre identité ou votre orientation.

Si vous vous reconnaissez dans l'un de ces signes, vous avez le droit de demander du soutien. Vous n'avez pas besoin d'attendre que la situation s'aggrave.

Ce qui vous arrive n'est pas votre faute. Ni parce que vous avez fait confiance, ni parce que vous avez partagé une photo, ni à cause de ce que vous portez, dites ou publiez, ni à cause de qui vous êtes ou de qui vous aimez. La responsabilité appartient entièrement à la personne qui vous fait du mal.

Protéger vos comptes

La plupart des piratages de comptes reposent sur un mot de passe faible ou réutilisé, un code volé, ou une personne proche qui connaît votre téléphone. Quelques changements font une grande différence.



Si une personne proche surveille peut-être vos comptes

Faites les changements depuis un appareil sûr auquel elle n'a pas accès. Lui couper l'accès d'un coup peut l'alerter. Si cela risque de vous mettre en danger, réfléchissez d'abord à votre plan de sécurité (chapitre 8) ou demandez du soutien.

1. Commencez par votre e-mail

Votre adresse e-mail est la clé principale : la personne qui la contrôle peut réinitialiser les mots de passe de tous vos autres comptes. Sécurisez-la en premier, puis les comptes liés à votre numéro de téléphone, puis les réseaux sociaux.

2. Des mots de passe solides et différents

- Utilisez une **phrase de passe** : au moins quatre mots choisis au hasard, faciles à retenir pour vous, difficiles à deviner. Par exemple : **olive-bus-nuage-riviere-27** (n'utilisez pas celle-ci !).
- **Ne réutilisez jamais** le même mot de passe sur deux comptes. Quand un site subit une fuite, les attaquants essaient ce mot de passe partout.
- Évitez les dates de naissance, les prénoms, les animaux, les numéros de téléphone : vos proches peuvent les deviner.
- Un **gestionnaire de mots de passe** (une application qui garde tous vos mots de passe dans un coffre chiffré, comme Bitwarden, ou celui intégré à votre téléphone ou à votre navigateur) rend tout cela simple. Vous n'avez plus qu'une seule phrase de passe solide à retenir.
- Ne donnez pas vos mots de passe à un-e partenaire, même « pour prouver votre confiance ». Les exiger peut être une forme de contrôle.

3. Activez la double authentification (2FA)

Avec la double authentification, une connexion depuis un nouvel appareil demande un second code en plus de votre mot de passe. Même si quelqu'un connaît votre mot de passe, cette personne ne peut pas entrer.

- **Le mieux** : une application d'authentification (Google Authenticator, Microsoft Authenticator, Aegis...) ou une clé d'accès (passkey).
- **Correct** : les codes par SMS. C'est mieux que rien, mais moins sûr, surtout si quelqu'un peut accéder à votre carte SIM ou à votre téléphone.

Plateforme	Où trouver le réglage
Facebook & Instagram	Paramètres → Espace Comptes → Mot de passe et sécurité → Authentification à deux facteurs → choisissez le compte → Application d'authentification (recommandé).

Plateforme	Où trouver le réglage
WhatsApp	Paramètres → Compte → Vérification en deux étapes → Activer → choisissez un code PIN à 6 chiffres que personne ne connaît → ajoutez une adresse e-mail pour pouvoir le réinitialiser.
Google / Gmail	Compte Google (myaccount.google.com) → Sécurité → Validation en deux étapes → suivez les étapes; ajoutez une application d'authentification et des codes de secours.
TikTok	Profil → menu ☰ → Paramètres et confidentialité → Sécurité → Validation en 2 étapes .

4. Gardez vos codes de récupération en lieu sûr

Quand vous activez la double authentification, la plateforme vous donne des **codes de récupération (codes de secours)**. Ils vous permettent de retrouver l'accès à votre compte si vous perdez votre téléphone. Notez-les ou imprimez-les, et rangez-les dans un endroit sûr, hors de portée de la personne qui vous fait du mal. N'envoyez jamais un code à qui que ce soit — même à quelqu'un qui se présente comme « l'assistance ».

5. Vérifiez qui est connecté

Regardez régulièrement les sessions et les appareils actifs, et déconnectez tout ce que vous ne reconnaissez pas :

- **Facebook / Instagram** : Espace Comptes → Mot de passe et sécurité → **Où vous êtes connecté-e**.
- **WhatsApp** : Paramètres → **Appareils connectés**. Un ordinateur connecté peut lire tous vos messages.
- **Google** : Compte Google → Sécurité → **Vos appareils**. Le **Check-up Sécurité** vous guide pas à pas.
- **TikTok** : Paramètres et confidentialité → Sécurité → **Gérer les appareils**.

Vérifiez aussi l'adresse e-mail et le numéro de téléphone de récupération de chaque compte, ainsi que les applications tierces qui y sont connectées. Supprimez tout ce qui n'est pas à vous.

6. Méfiez-vous des liens et de la fausse « assistance »

Ne saisissez jamais votre mot de passe sur une page ouverte depuis un lien reçu par message, même si elle a l'air officielle. Ouvrez l'application ou tapez l'adresse vous-même. Les plateformes ne demandent jamais votre code ni votre mot de passe par message.



Astuce

Un compte par jour : d'abord l'e-mail, puis WhatsApp, puis Facebook/Instagram, puis le reste.
Un petit pas reste un pas.

Votre téléphone et vos appareils

Votre téléphone contient vos messages, vos photos, votre localisation et vos comptes. Une personne qui l'a entre les mains, même quelques minutes, peut faire beaucoup. Voici comment le protéger.

Verrouillage de l'écran

- Utilisez un code PIN d'au moins 6 chiffres ou un mot de passe. Évitez les schémas simples et les dates.
- Soyez prudent·e avec le déverrouillage par empreinte ou par visage si quelqu'un pourrait vous y forcer, ou l'utiliser pendant votre sommeil.
- Ne donnez pas votre code. Si quelqu'un le connaît déjà, changez-le.
- Masquez le contenu des notifications sur l'écran verrouillé, pour que vos messages et vos codes ne puissent pas être lus sans déverrouiller le téléphone.

Les applications que vous ne reconnaissez pas

Parcourez la liste complète des applications (Paramètres → Applications). Certaines applications espionnes se cachent derrière des noms banals comme « Service système » ou « Sync ». Vérifiez aussi :

- **Android** : Paramètres → Sécurité → **Applis d'administration de l'appareil**, ainsi que les applications qui ont accès à l'Accessibilité, aux notifications ou à la localisation. Vérifiez que **Google Play Protect** est activé.
- **iPhone** : Réglages → Général → **VPN et gestion de l'appareil** (profils inconnus). Le **Contrôle de sécurité** (Réglages → Confidentialité et sécurité) montre avec qui vous partagez des accès et vous permet d'y mettre fin.

Les signes d'un logiciel espion (stalkerware)

- Quelqu'un connaît vos messages, vos conversations ou vos déplacements sans que vous lui en ayez parlé.
- La batterie se vide anormalement vite, ou le téléphone chauffe quand vous ne l'utilisez pas.
- La consommation de données mobiles augmente sans raison.
- Des réglages ont changé sans vous (localisation activée, paramètres de sécurité désactivés).
- La personne a eu votre téléphone entre les mains, ou vous l'a « configuré ».



Ne supprimez pas tout de suite une application espionne

Si vous soupçonnez un logiciel espion, le supprimer peut alerter la personne et rendre la situation plus dangereuse. Cela efface aussi des preuves. Faites d'abord un plan de sécurité (chapitre 8), demandez de l'aide depuis un autre appareil et faites-vous accompagner sur le plan technique. Quand vous êtes en sécurité, une réinitialisation complète (retour aux paramètres d'usine) — après avoir sauvegardé vos preuves — est le nettoyage le plus fiable.

Le partage de position

- Vérifiez si vous partagez votre position dans **Google Maps** (Partage de position), dans **Localiser** sur iPhone (Partager ma position), sur **Snapchat** (Snap Map — activez le mode Fantôme) et dans les

applications de suivi familial.

- Désactivez la localisation pour les applications qui n'en ont pas besoin (Paramètres → Localisation / Confidentialité → Service de localisation).
- Évitez de publier votre position en temps réel. Publiez après avoir quitté un lieu.

Les traceurs physiques

De petits traceurs Bluetooth (de type AirTag) peuvent être cachés dans un sac, un manteau ou une voiture.

- L'**iPhone** vous prévient quand un traceur inconnu se déplace avec vous (alerte « AirTag détecté près de vous » — en anglais « AirTag Found Moving With You »).
- **Android** propose les **Alertes de traceurs inconnus** (Paramètres → Sécurité et urgences) et une recherche manuelle.
- Si vous en trouvez un, pensez à votre sécurité avant de le retirer : la personne pourrait s'en rendre compte. Prenez-le en photo, notez où et quand vous l'avez trouvé, et demandez du soutien.

Les photos en disent plus que vous ne le pensez

Les photos peuvent contenir des informations cachées (métadonnées) : le lieu et l'heure exacts de la prise de vue. Désactivez la géolocalisation dans les réglages de l'appareil photo. Pour partager depuis un iPhone, touchez **Options** et désactivez **Position** ; dans Google Photos, utilisez **Supprimer la position** (Remove location). Regardez aussi l'arrière-plan : un panneau de rue, un uniforme scolaire ou la vue depuis une fenêtre peuvent révéler où vous êtes.

Sauvegardes et cloud

Vos photos et vos messages sont souvent copiés sur **iCloud**, **Google Photos / Google Drive** ou dans une sauvegarde WhatsApp. Toute personne qui connaît le mot de passe de ce compte peut tout voir, depuis n'importe quel appareil. Sécurisez ces comptes comme expliqué au chapitre 3, et vérifiez quels appareils y sont connectés.

Mises à jour

Installez régulièrement les mises à jour du système et des applications. Elles corrigent des failles de sécurité que les attaquants utilisent.



Téléphone partagé ou d'occasion ?

Si on vous a donné le téléphone, ou si quelqu'un d'autre l'a configuré, cette personne a peut-être encore accès à ses comptes. Connectez-vous avec une nouvelle adresse e-mail à vous, et vérifiez partout les « Appareils connectés » et les appareils associés.

Les paramètres de confidentialité, plateforme par plateforme

Les paramètres de confidentialité décident qui peut vous voir, vous contacter et vous trouver. Dix minutes par plateforme suffisent.

Les noms des menus changent selon les versions et les langues des applications. Si vous ne trouvez pas un réglage, tapez son nom dans la barre de recherche des paramètres de l'application.

Facebook

- ☐ Lancez l'**Assistance confidentialité** (Paramètres et confidentialité) : elle vous guide étape par étape.
- ☐ Réglez vos futures publications sur **Amis**, pas sur Public. Utilisez **Limiter les anciennes publications** pour les plus anciennes.
- ☐ Masquez votre liste d'amis, votre numéro de téléphone, votre e-mail et votre date de naissance.
- ☐ Activez l'**examen des identifications** et l'**examen du profil** (Tag review, Profile review), pour que rien n'apparaisse sur votre profil sans votre accord.
- ☐ Limitez qui peut vous envoyer des invitations et qui peut vous trouver avec votre numéro de téléphone ou votre e-mail.
- ☐ Utilisez **Bloquer** pour les comptes malveillants, et **Restreindre** si vous ne voulez pas que la personne le sache.

Instagram

- ☐ Passez en **Compte privé**.
- ☐ Utilisez **Restreindre** (la personne ne le saura pas) ou **Bloquer** pour les comptes problématiques — y compris les nouveaux comptes qu'elle pourrait créer.
- ☐ Choisissez qui peut vous envoyer des messages, commenter, vous identifier et vous mentionner.
- ☐ Activez les **Mots masqués** pour filtrer les commentaires et les demandes de messages offensants.
- ☐ Utilisez les **Limites** pour masquer temporairement les commentaires et les messages des comptes qui ne vous suivent pas ou qui vous suivent depuis peu. C'est utile pendant une attaque.
- ☐ Utilisez **Amis proches** pour les stories personnelles, et masquez votre statut d'activité.

WhatsApp

- ☐ Paramètres → Confidentialité: choisissez qui voit votre **Vu à et en ligne**, votre **Photo de profil**, votre **Infos** et votre **Statut**.
- ☐ **Groupe**s: « Mes contacts » uniquement, pour que des inconnu·es ne puissent pas vous ajouter.
- ☐ **Appels** → **Mettre en silence les appels inconnus**.
- ☐ Vérifiez régulièrement les **Appareils connectés**.
- ☐ La **Vérification de confidentialité** (Privacy checkup, dans Paramètres → Confidentialité) regroupe tout cela au même endroit.
- ☐ À savoir: les messages éphémères et les médias « à vue unique » n'empêchent pas quelqu'un de photographier l'écran.

TikTok

- ☐ Passez en **Compte privé**.
- ☐ Désactivez **Suggérer votre compte à d'autres personnes** (y compris aux contacts et aux amis Facebook).
- ☐ Choisissez qui peut commenter, faire un **Duo** ou un **Collage** (Stitch), télécharger vos vidéos et vous envoyer des messages.
- ☐ Utilisez les **filtres** de commentaires et les filtres par mots-clés.
- ☐ Masquez votre statut d'activité et les comptes que vous suivez.



Faites une « recherche sur vous-même »

Cherchez votre nom, votre nom d'utilisateur et votre numéro de téléphone dans un moteur de recherche et sur chaque plateforme, déconnecté·e ou depuis l'appareil d'une personne de confiance. Vous verrez ce que voient les inconnu·es.

Si cela arrive: fiches réflexes

Des fiches courtes et pratiques pour les situations les plus fréquentes. Lisez celle dont vous avez besoin. Dans tous les cas: ce n'est pas votre faute, vous pouvez garder des preuves avant de bloquer, et vous pouvez demander du soutien à chaque étape.

6.1 Mon compte a été piraté

Les signes: des messages que vous n'avez pas envoyés, un mot de passe modifié, vous ne pouvez plus vous connecter.

- 1 **Essayez de le récupérer** avec les outils officiels: Facebook facebook.com/hacked · Instagram instagram.com/hacked · Google/Gmail g.co/recover · WhatsApp: enregistrez de nouveau votre numéro sur votre téléphone, ce qui déconnecte l'autre personne, puis activez la vérification en deux étapes.
- 2 **Une fois le compte récupéré**: choisissez un nouveau mot de passe solide, changez aussi celui de votre e-mail, déconnectez toutes les sessions inconnues, activez la double authentification, vérifiez l'e-mail et le téléphone de récupération ainsi que les applications connectées.
- 3 **Prévenez vos contacts** de ne pas répondre aux messages qui demandent de l'argent, des photos ou des codes.
- 4 **Gardez des preuves**: captures d'écran des messages envoyés en votre nom et des modifications du compte.

Si la personne qui est entrée dans votre compte est un-e proche qui a accès à votre téléphone, faites tout cela depuis un autre appareil, sûr.

6.2 On me menace

- 1 **Évaluez le risque**. La personne sait-elle où vous habitez, travaillez ou étudiez? Les menaces parlent-elles de violence physique? Deviennent-elles plus fréquentes? Si la réponse est oui à l'une de ces questions, prenez-le au sérieux: appelez le **1899**, ou la police au **197** si le danger est proche.
- 2 **Ne répondez pas, ne provoquez pas**. Répondre peut faire monter la tension.
- 3 **Gardez des preuves de tout** (chapitre 7) et conservez les messages d'origine, même après avoir bloqué.
- 4 **Bloquez et signalez** le compte à la plateforme une fois les preuves sauvegardées.
- 5 **Préparez votre sécurité**: prévenez une personne de confiance, changez vos trajets et vos horaires si la personne les connaît, désactivez le partage de position.

6.3 On me fait du chantage ou de la sextorsion

Ce qui s'est passé n'est pas votre faute. La responsabilité appartient entièrement à la personne qui vous fait du chantage.

- 1 **Ne payez pas et n'envoyez pas d'autres images.** Payer arrête rarement le chantage ; cela entraîne souvent de nouvelles exigences.
- 2 **Ne supprimez pas la conversation.** Faites des captures d'écran qui montrent le nom du compte, son lien et la date.
- 3 **Coupez le contact** une fois les preuves gardées. Ne négociez pas. Vous pouvez désactiver votre compte temporairement au lieu de le supprimer.
- 4 **Sécurisez vos comptes :** changez vos mots de passe, activez la double authentification, passez vos profils en privé, masquez vos listes d'amis et d'abonné-es.
- 5 **Signalez le compte** à la plateforme : elles ont des procédures dédiées aux images intimes.
- 6 **Protégez vos images** avec StopNCII.org ou Take It Down (voir 6.4).
- 7 **Parlez-en** à une personne de confiance, et demandez du soutien.

6.4 Mes images intimes ont été diffusées (ou risquent de l'être)

Que vous ayez envoyé une image en toute confiance, que l'on vous ait filmé-e à votre insu, ou qu'un faux ait été fabriqué par IA : dans tous les cas, ce n'est pas votre faute.

- 1 **Notez où l'image apparaît** (lien, compte, date) sans la partager de nouveau.
- 2 **Signalez-la à la plateforme** avec l'option prévue pour les images intimes partagées sans consentement. Les plateformes traitent ces signalements en priorité.
- 3 **StopNCII.org** (si vous aviez 18 ans ou plus sur l'image) : crée une « empreinte » numérique (hash) de vos images sur votre propre appareil — l'image elle-même n'est jamais envoyée — pour que les plateformes partenaires puissent la bloquer.
- 4 **Take It Down** (takeitdown.ncmec.org) : le même principe si vous aviez moins de 18 ans sur l'image.
- 5 **Moteurs de recherche :** Google propose un formulaire officiel pour demander le retrait des images intimes non consenties de ses résultats de recherche.
- 6 **Demandez du soutien**, psychologique et juridique. Vous n'êtes pas seul-e.

! N'envoyez jamais les images

N'envoyez d'images intimes à personne pour « prouver » ce qui s'est passé — ni à nous, ni à qui que ce soit. Une description et le lien de la publication suffisent.

6.5 Être outé-e, ou menacé-e d'outing

Votre identité vous appartient. Vous seul-e décidez qui la connaît, et quand.

En Tunisie, être outé-e peut entraîner un rejet familial, la perte d'un logement ou d'un emploi, des violences physiques ou des problèmes judiciaires. Nous considérons cette situation comme potentiellement dangereuse.

Si quelqu'un menace de vous outter

- 1 **Ne payez pas, n'envoyez rien.** C'est du chantage ; payer ne l'arrête pas.

- 2 **Gardez une trace** de la menace et conservez les preuves dans un endroit sûr — pas sur un téléphone partagé.
- 3 **Réduisez ce que l'on peut trouver sur vous**: faites le tri dans vos comptes, masquez vos listes d'amis, retirez les photos qui pourraient être utilisées, et vérifiez vos autres comptes (applications de rencontre, anciens profils, discussions de groupe).
- 4 **Faites un plan de sécurité**: où pourriez-vous aller si la situation devient difficile à la maison ? Qui pourriez-vous appeler ? Qu'emporteriez-vous ? (chapitre 8)
- 5 **Demandez du soutien** à des personnes et à des organisations qui respectent les personnes LGBTQI+. E-RADAR peut vous aider à les trouver.

Si vous avez été outé-e

- Votre sécurité physique passe avant tout. Si vous êtes en danger, appelez le **197** ou le **193**, ou rejoignez une personne ou un lieu sûrs.
- Signalez les publications : révéler l'orientation ou l'identité de quelqu'un est contraire aux règles de la plupart des plateformes.
- Le soutien psychologique compte beaucoup en ce moment. Vous n'êtes pas seul-e.

Avant d'envisager de vous adresser aux autorités, faites-vous accompagner sur le plan juridique pour comprendre les risques et vos options.

6.6 Une campagne de haine en ligne contre moi

Insultes ou moqueries sur votre genre, votre corps, votre identité ou votre orientation ; appels à la violence ; de nombreux comptes qui attaquent en même temps pour vous faire taire.

- 1 **Ne lisez pas tout vous-même**. Demandez à une personne de confiance de trier et de garder les preuves pour vous.
- 2 **Gardez des preuves** des publications et des comptes, surtout ceux qui contiennent des menaces, des incitations ou vos informations personnelles.
- 3 **Utilisez les outils des plateformes**: filtres par mots-clés, limitation des commentaires, Restreindre ou Bloquer, les « Limites » d'Instagram.
- 4 **Signalez**: les plateformes interdisent les discours de haine fondés sur le genre, l'identité et l'orientation.
- 5 **Faites une pause**: passez votre compte en privé ou désactivez-le temporairement, le temps que les choses se calment.

Si l'attaque contient des menaces ou votre adresse, suivez aussi la fiche 6.2.

La haine en dit long sur la personne qui l'écrit, pas sur vous.

6.7 On me traque en ligne

Les signes : des messages ou des appels répétés alors que vous avez dit stop ; de nouveaux comptes à chaque fois que vous bloquez ; la personne sait où vous étiez ou avec qui ; des cadeaux ou des messages qui arrivent là où vous allez.

Comment elle peut savoir où vous êtes: le partage de position dans une application, un logiciel espion sur votre téléphone, un traceur physique dans vos affaires ou votre voiture, ou des indices de lieu dans vos publications ou celles de vos ami·es.

- 1 **Notez chaque incident** dans votre journal (chapitre 7): date, heure, ce qui s'est passé.
- 2 **Vérifiez et désactivez le partage de position** (chapitre 4).
- 3 **Si vous soupçonnez une application espionne, ne la supprimez pas tout de suite**: la personne pourrait s'en apercevoir. Demandez d'abord un accompagnement technique.
- 4 **Parlez-en à une personne de confiance** et faites un plan de sécurité.



La traque peut devenir un danger physique

Si vous vous sentez en danger, appelez le **197** (police), le **193** (garde nationale) ou le **1899**.

Garder et conserver les preuves

Garder des preuves ne vous engage à rien. Mais si un jour vous voulez signaler ou porter plainte, elles seront là.

Ce qu'il faut garder

- ☐ Des captures d'écran des messages, des commentaires ou des publications, **avec la date et l'heure visibles**.
- ☐ Le **nom du compte et son lien** (URL du profil ou @nomdutilisateur) — pas seulement le nom affiché, qui peut changer.
- ☐ Les liens des publications, des vidéos ou des pages.
- ☐ L'historique des appels et les SMS.
- ☐ Les e-mails, avec l'adresse de l'expéditeur.
- ☐ Un court résumé: ce qui s'est passé, quand, où, qui l'a vu.

Comment faire de bonnes captures d'écran

- Vérifiez que la capture montre le nom du compte, la date et l'heure, et le message en entier.
- Pour un profil, capturez la page avec son URL visible (sur ordinateur, la barre d'adresse).
- Pour une longue conversation, faites plusieurs captures qui se chevauchent, dans l'ordre.
- Sur WhatsApp, vous pouvez aussi **exporter la discussion** (Discussion → Plus → Exporter la discussion) et garder le fichier exporté.
- Certaines plateformes vous permettent de **télécharger vos données** (Facebook, Instagram, Google Takeout), messages compris.

Comment conserver les preuves en sécurité

- Rangez-les hors de portée de la personne qui vous fait du mal — pas sur un téléphone partagé ni sur un compte cloud partagé.
- Gardez une **deuxième copie** dans un autre endroit sûr (une clé USB, une adresse e-mail séparée que vous seul-e connaissez, une personne de confiance).
- Ne modifiez pas, ne recadrez pas et n'ajoutez pas les fichiers d'origine. Faites des copies si besoin.
- Donnez aux fichiers des noms clairs: **2026-03-14_instagram_@compte_menace.png**.



Garder des preuves peut faire mal

Revoir des contenus violents est difficile. Vous pouvez demander à une personne de confiance de le faire avec vous ou à votre place. Faites des pauses.



Images intimes

N'envoyez d'images intimes à personne comme preuve. Notez le lien et une description; les professionnel·les vous diront comment procéder en toute sécurité.

Journal des incidents

Remplissez une ligne par incident. Gardez cette fiche dans un endroit sûr. Faites-en autant de copies que nécessaire.

Date	Heure	Plateforme	Compte / lien	Ce qui s'est passé	Capture d'écran rangée où ?	Témoins

Exemple : 14/03 · 22h10 · Instagram · @compte_exemple (instagram.com/compte_exemple) · A menacé d'envoyer mes photos à mon frère · Clé USB, dossier « Mars » · Mon amie S. a vu le message.

Mon plan de sécurité personnel

Un plan de sécurité, ce sont des décisions que vous prenez à l'avance, au calme, pour savoir quoi faire si la situation s'aggrave. Remplissez-le sur papier, seul-e ou avec une personne de confiance. Gardez-le caché, ou gardez-le en tête.



Gardez ce plan en lieu sûr

Si la personne qui vous fait du mal vit avec vous ou fouille vos affaires, ne laissez pas cette page là où elle pourrait la trouver. Vous pouvez en confier une copie à une personne de confiance.

Les personnes de confiance

que je peux appeler ou rejoindre, à tout moment

Les lieux sûrs

où je peux aller si je dois partir vite

Mot de code

un mot ou un emoji qui dit à mes personnes de confiance « J'ai besoin d'aide, appelle / viens maintenant »

Appareil sûr

un téléphone ou un ordinateur auquel la personne n'a pas accès

Comptes sûrs

une adresse e-mail que je suis seul-e à connaître, pour l'aide et les preuves

Où sont rangées mes preuves

et qui en a une deuxième copie

Ce que j'emporterais

si je devais partir

☐ carte d'identité / passeport · ☐ téléphone et chargeur · ☐ argent / carte bancaire · ☐ clés · ☐ médicaments · ☐ documents importants · ☐ ce plan et mes codes de récupération · ☐ un objet qui me réconforte

Numéros d'urgence

1899 numéro vert pour les femmes victimes de violence · **197** police · **193** garde nationale · **190** SAMU

Repères juridiques en Tunisie

Ce chapitre donne des informations générales pour vous aider à comprendre vos droits. Ce n'est pas un conseil juridique, et cela ne remplace pas une consultation avec un·e avocat·e ou un·e professionnel·le du droit qualifié·e.

Loi organique n° 2017-58 relative à l'élimination de la violence à l'égard des femmes

Cette loi reconnaît plusieurs formes de violence à l'égard des femmes : physique, morale (psychologique), sexuelle, économique et politique. Elle donne aux victimes des droits à la protection, à l'information et à l'orientation, ainsi qu'à un accompagnement juridique et psychologique.

Loi organique n° 2004-63 portant sur la protection des données à caractère personnel

Cette loi protège vos données personnelles. Publier vos informations ou vos images sans votre consentement peut être contraire à la loi.

À qui vous adresser

- Le numéro vert **1899** pour les femmes victimes de violence.
- Les unités spécialisées dans les enquêtes sur les violences à l'égard des femmes, au sein de la police et de la garde nationale.
- Les associations qui proposent un accompagnement et une aide juridique gratuits.

Avant de décider

- Gardez d'abord des preuves (chapitre 7) : de bonnes preuves aident dans toute démarche.
- Vous pouvez vous faire accompagner par une personne de confiance ou par un·e professionnel·le du droit.
- Demandez ce qui va se passer ensuite, qui sera informé, et comment vos informations seront protégées.



En toute honnêteté

Nous savons que certaines personnes — en particulier les personnes LGBTQI+ — peuvent avoir peur de s'adresser aux autorités, et que cette peur peut être fondée. Aller à la police ou devant la justice reste toujours votre choix. Un accompagnement juridique peut vous aider à comprendre les risques et les options avant de décider. Et certaines démarches (garder des preuves, signaler aux plateformes, protéger vos images) ne demandent aucune procédure officielle.

Avertissement : les informations de ce chapitre sont générales et peuvent évoluer. Elles ne constituent pas un conseil juridique. Pour votre situation, consultez un·e avocat·e ou un service d'aide juridique. Intersection Association ne peut être tenue responsable des décisions prises sur la seule base de ce guide.

Prendre soin de vous

La violence numérique ne reste pas sur l'écran. Elle touche le sommeil, l'humeur, la concentration et les relations. Prendre soin de vous fait partie de votre protection.

Des réactions normales

Après une violence numérique, beaucoup de personnes ressentent : de la peur à chaque vibration du téléphone, de la honte ou de la culpabilité, de l'anxiété, des difficultés à dormir, l'envie de s'isoler, ou de la colère. Certaines se sentent comme anesthésiées. Ce sont des réactions normales face à une situation qui, elle, ne l'est pas.

Des petites choses qui aident

Moins d'écran

Limitez le temps passé à lire les commentaires ou les messages. Laissez une personne de confiance les regarder pour vous.

Moins d'alertes

Coupez les notifications des applis qui vous stressent, masquez certains mots ou comptes.

Une routine simple

Dormir, manger, bouger un peu. Les petites habitudes régulières redonnent un sentiment de contrôle.

Quelqu'un à qui parler

Parlez à une personne de confiance. Vous n'êtes pas obligé-e de tout raconter.

Pensez à ce qui vous fait vous sentir en sécurité : un lieu, une personne, une activité, une musique. Notez-le dans votre plan de sécurité.

À quoi ressemble un soutien psychologique

- Une personne formée vous écoute sans vous juger.
- Vous choisissez de quoi parler, à votre rythme.
- Elle vous aide à comprendre ce que vous ressentez et à faire face au stress.
- Tout reste confidentiel, avec votre accord.

Vous pouvez demander un soutien psychologique via E-RADAR : e-radar.intersection.uno/fr/support/

Si vous soutenez quelqu'un

- Croyez la personne. Dites-lui : « Ce n'est pas ta faute. »
- Écoutez plus que vous ne conseillez. Laissez-la décider.
- Ne partagez pas son histoire ni ses images, même « pour aider ».
- Proposez une aide concrète : garder des preuves, être à ses côtés pendant un signalement, chercher des informations.
- Prenez soin de vous aussi.



Si vous pensez à vous faire du mal

Parlez-en à quelqu'un maintenant, s'il vous plaît : une personne de confiance, ou appelez le SAMU au **190**. Vous méritez de l'aide et du soutien.

Où trouver de l'aide

Vous n'êtes pas seul-e. Voici qui vous pouvez contacter.

1899

Numéro vert pour les
femmes victimes de
violence

197

Police

193

Garde nationale

190

SAMU — urgence
médicale

E-RADAR — e-radar.intersection.uno

Une plateforme confidentielle d'Intersection Association, en darija, en français et en anglais.

Signaler un incident	Racontez ce qui s'est passé, de façon anonyme si vous le souhaitez. /fr/report/
Demander de l'aide	Soutien psychologique, juridique ou technique. /fr/support/
Suivre avec votre code	Après l'envoi, vous recevez un code de suivi. Gardez-le en lieu sûr: il vous permet de suivre votre signalement sans donner votre nom. /fr/track/
En danger maintenant ?	Ce qu'il faut faire tout de suite. /fr/danger/
Ressources	Des fiches courtes sur chaque thème de ce guide. /fr/resources/

Vous avez perdu votre code de suivi ? Il ne peut pas être récupéré, mais vous pouvez toujours envoyer un nouveau signalement ou une nouvelle demande.

Pages d'aide des plateformes

- Comptes piratés: facebook.com/hacked · instagram.com/hacked · g.co/recover
- Images intimes: StopNCII.org · takeitdown.ncmec.org

Organisations de confiance près de chez moi

À remplir par Intersection ou par vous : les organisations, les services et les personnes vers qui vous tourner près de chez vous.

Nom	Ce qu'elles proposent	Contact

Listes de vérification d'une page

Cochez au fur et à mesure. Vous n'avez pas besoin de tout faire d'un coup.

Sécurité des comptes

- ☐ Mon e-mail a une phrase de passe solide et unique, et la double authentification.
- ☐ Chaque compte important a son propre mot de passe (ou j'utilise un gestionnaire de mots de passe).
- ☐ La double authentification est activée: Facebook/Instagram, WhatsApp (code PIN), Google, TikTok.
- ☐ Mes codes de récupération sont notés et rangés en lieu sûr.
- ☐ J'ai vérifié les sessions actives et déconnecté les appareils inconnus.
- ☐ L'e-mail et le numéro de téléphone de récupération sont à moi et à jour.
- ☐ J'ai supprimé les applications connectées que je n'utilise pas.
- ☐ Personne d'autre ne connaît mes mots de passe ni mes codes.

Mon téléphone

- ☐ Écran verrouillé avec un code PIN d'au moins 6 chiffres que personne ne connaît.
- ☐ Contenu des notifications masqué sur l'écran verrouillé.
- ☐ J'ai passé en revue mes applications et leurs autorisations (localisation, micro, accessibilité).
- ☐ Le partage de position est désactivé là où je n'en ai pas besoin (Maps, Localiser, Snap Map).
- ☐ La géolocalisation de l'appareil photo est désactivée.
- ☐ Mon compte cloud (iCloud / Google) est sécurisé et je sais quels appareils y sont connectés.
- ☐ « Appareils connectés » vérifiés sur WhatsApp.
- ☐ Le système et les applications sont à jour.

Si l'on me fait du chantage

- ☐ Je ne paie pas et je n'envoie rien de plus.
- ☐ Je ne supprime pas la conversation.
- ☐ J'ai fait des captures d'écran avec le nom du compte, le lien et la date.
- ☐ J'ai arrêté de répondre une fois les preuves gardées.
- ☐ J'ai changé mes mots de passe et activé la double authentification.
- ☐ J'ai passé mes comptes en privé et masqué mes listes d'amis et d'abonné-es.
- ☐ J'ai signalé le compte à la plateforme.
- ☐ J'ai utilisé StopNCII.org / Take It Down si des images sont en jeu.
- ☐ J'en ai parlé à une personne de confiance.
- ☐ Je connais les numéros : **1899 · 197 · 193 · 190**.

Ce n'est pas votre faute. Vous n'êtes pas seul-e.



Vous n'êtes pas seul·e. Nous sommes à vos côtés.

E-RADAR est une plateforme confidentielle d'Intersection Association pour les femmes, les filles et les personnes LGBTQI+ confrontées aux violences numériques fondées sur le genre en Tunisie.

e-radar.intersection.uno

1899 · 197 · 193 · 190

Ce guide donne des informations générales. Ce n'est pas un conseil juridique, médical ou technique adapté à votre situation particulière. Les noms des menus des applications changent avec le temps. Édition 2026.