

GUIDE

Protection numérique pour personnes victimes de violences



Comprendre et suivre les étapes pour se protéger
numériquement, pas à pas.





Règle d'or

Effectue toutes ces démarches depuis un appareil et un réseau Wi-Fi que l'agresseur ne connaît pas (données mobiles personnelles ou réseau d'un tiers de confiance).

1. Sécurise tes comptes

👉 Faire ceci depuis un appareil sûr, en dehors du domicile.

Mots de passe

- Change tous tes mots de passe immédiatement
 - > Tu peux utiliser un gestionnaire (Proton Pass, etc.)
- **Ne réutilise jamais un mot de passe connu de l'agresseur**
- Choisis une nouvelle adresse email principale inconnue (sur ProtonMail par exemple)

Mets en place la double authentification (2FA)

- Active, sur chaque compte, via une app : Aegis (Android) ou Authy
- **Évite la 2FA par SMS si le numéro est accessible à l'agresseur**
- **Vérifie et révoque les sessions actives (appareils connectés) sur chaque compte**

Comptes prioritaires

1. Adresse email principal
2. Apple ID / Compte Google
3. Banque, PayPal
4. Opérateur téléphonique (change le code PIN SIM)
5. Réseaux sociaux
6. Tout service lié à ta localisation ou tes enfants

Vérifie les accès tiers

- Google : Mon compte > Sécurité > Accès des applications tierces
- Apple : Réglages > [Ton nom] > Partage familial & appareils connectés
- **Révoquer tout accès non reconnu**

Vérifie les applications et leurs autorisations

Prends quelques minutes pour vérifier quelles applications ont accès à ton téléphone ou à tes comptes.

Contrôle notamment :

- Les applications que tu ne reconnais pas ou que tu n'utilises plus.
- Les autorisations accordées (localisation, microphone, caméra, contacts, SMS, photos...).
- Les applications ayant accès à ton compte Google ou Apple.
- Les applications disposant des droits d'accessibilité ou d'administration de l'appareil (Android).

Supprime les applications suspectes et retire les autorisations qui ne sont pas nécessaires.

 **Les logiciels espions utilisent souvent des autorisations très étendues pour accéder à tes données sans que tu t'en rendes compte.**

2. Détecte et supprime les logiciels espions

Signes d'alerte

- Batterie qui se vide vite, téléphone chaud au repos, consommation data anormale
- L'agresseur connaît des détails de conversations privées

Actions

- Vérifie la liste des applications installées et désinstalle toute application inconnue ou suspecte.
- iPhone : mettre à jour iOS, réinitialiser les réglages réseau, vérifier Localisation > Partager ma position
- Android : vérifier Paramètres > Applications > Accès spéciaux, désactiver les sources inconnues
- En cas de doute sérieux : réinitialisation d'usine (sauvegarder photos/contacts avant)
- Vérifier les AirTags / trackers Bluetooth (app Détecteur de traqueurs sur Android)

3. Efface ton historique pour ne laisser aucune trace

Sur navigateur (Chrome, Firefox, Safari)

- Supprimer **historique, cookies, cache, mots de passe enregistrés**
- Chrome : ☰ > Paramètres > Confidentialité > Effacer les données
- **Toujours utiliser la navigation privée** sur un appareil partagé
- Désactiver la synchronisation du compte Google/Apple si l'agresseur y a accès

Sur téléphone

- Effacer l'historique des appels et SMS suspects
- Vider la liste de suggestions du clavier (souvent oubliée)
- Nettoyer l'historique de recherche vocale (Siri, Google Assistant, Alexa)
- Supprimer les recherches récentes dans Maps / Google Maps
- Vider la corbeille des photos après suppression

Sur les comptes en ligne

- Effacer l'historique d'activité Google : myactivity.google.com
- Désactiver "Activité Web et App" dans les paramètres Google
- Supprimer l'historique d'écoute/visionnage (Spotify, Netflix, YouTube)
- Vider l'historique de recherche sur chaque réseau social

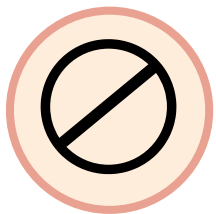
Traces souvent oubliées

- Historique **iCloud / Google Drive** (documents récents)
- **Suggestions de contacts** dans l'appli mail
- **Routeur Wi-Fi domestique** : l'agresseur peut consulter les sites visités s'il a accès à la box — *utiliser les données mobiles ou un réseau extérieur pour toute démarche sensible*

4. Maîtrise ta localisation



DÉSACTIVER LE PARTAGE DE POSITION (GOOGLE MAPS, FIND MY, SNAPCHAT, WHATSAPP)



COUPER LE GPS QUAND INUTILE



DÉSACTIVER LE WI-FI ET BLUETOOTH EN DÉPLACEMENT SENSIBLE



VÉRIFIER QUE LES PHOTOS ENVOYÉES NE CONTIENNENT PAS DE MÉTADONNÉES GPS

> Activer "Retirer la localisation" avant d'envoyer

5. Communiquer en sécurité

Besoin	Outil recommandé
Messagerie sécurisée	Signal (messages éphémères activés)
Email anonyme	ProtonMail
Navigation discrète	Firefox + mode privé
Appels anonymes	Carte SIM prépayée (achat en cash)

👉 Crée une adresse email inconnue de l'agresseur pour toutes les démarches administratives.

6. Sécurise tes données



Sauvegarder photos et documents importants sur un compte cloud inconnu de l'agresseur



Activer le verrouillage automatique + code PIN long (pas biométrie si risque de déverrouillage forcé)



Supprimer l'historique de navigation régulièrement



Sur ordinateur partagé : toujours utiliser la navigation privée, se déconnecter de tous les comptes

7. Réseaux sociaux



Passer tous les profils en privé



Retirer l'adresse, lieu de travail, école des enfants de la bio



Ne pas publier de photos géolocalisées ni révélant un nouveau lieu de vie



Bloquer l'agresseur et ses proches susceptibles de relayer des informations



Désactiver la synchronisation des contacts pour éviter d'être suggéré·e

8. Collecte des preuves numériques



Faire des captures d'écran de messages, appels, harcèlement en ligne (inclure la date/heure visible)



Sauvegarder sur un espace sécurisé hors de portée



Ne pas supprimer les messages menaçants avant de les avoir sauvegardés



Conserver les numéros d'expéditeurs inconnus

7. Contacts



17

Police/ Gendarmerie



114

SMS – accessible sans parler



3919

Violences Femmes Info
écoute anonyme et gratuite



police-nationale.interieur.gouv.fr

Signalement en ligne



cybermalveillance.gouv.fr

Aide aux victimes de cyberviolences



arretonslesviolences.gouv.fr

Formulaire de signalement discret

Checklist – ce que j’ai fait pour me protéger

Mon téléphone

- ☐ Code PIN changé (pas biométrie)
- ☐ Verrouillage automatique activé
- ☐ Localisation / partage de position désactivé
- ☐ Applications espionnes vérifiées / supprimées
- ☐ Trackers Bluetooth vérifiés (AirTag, etc.)
- ☐ Historique des appels et SMS nettoyé
- ☐ Suggestions du clavier effacées
- ☐ Corbeille des photos vidéo

Mes comptes

- ☐ Nouvelle adresse email créée (ProtonMail)
- ☐ Tous les mots de passe changés
- ☐ 2FA activée sur chaque compte important
- ☐ Sessions actives / appareils connectés révoqués
- ☐ Accès tiers vérifiés et révoqués
- ☐ Code PIN SIM changé

Ma navigation

- ☐ Historique, cookies, cache supprimés
- ☐ Navigation privée activée sur appareil partagé
- ☐ Synchronisation du compte navigateur désactivée
- ☐ Activité Google effacée (myactivity.google.com)
- ☐ Historique Maps / recherche vocale supprimé
- ☐ Routeur domestique évité pour démarches sensibles

Mes réseaux sociaux

- ☐ Profils passés en privé
- ☐ Agresseur + entourage bloqués
- ☐ Infos de localisation retirées du profil
- ☐ Synchronisation des contacts désactivée
- ☐ Historique de recherche nettoyé

Mes communications

- ☐ Signal installé avec messages éphémères
- ☐ Numéro / SIM prépayée si besoin
- ☐ Démarches admin sur nouvelle adresse email

J'ai noté ces numéros

- ☐ 3919 — Violences Femmes Info
- ☐ 17 — Police / Urgence
- ☐ cybermalveillance.gouv.fr
- ☐ Un·e proche de confiance : _____

**Chaque case cochée est un pas vers la sécurité.
Tu n'as pas à tout faire en une fois.**

**Avance à ton rythme.
Tu mérites d'être en sécurité et
entouré·e.**



⚠ À savoir : Ce guide donne des repères généraux. Il ne remplace pas un accompagnement personnalisé.