toutsurlacyber .fr

Fiche pratique gratuite · novembre 2026

Après une rupture : reprendre le contrôle de son téléphone et de ses comptes

Les réglages à vérifier, dans l'ordre, en une heure environ. **Vous n'êtes pas seule** : des personnes sont là pour vous aider à chaque étape.

Cochez chaque case au fur et à mesure. Gardez cette fiche dans un endroit sûr.

Votre sécurité d'abord

- Si la séparation se passe mal, couper un accès peut alerter l'autre personne. Avant de changer vos réglages, appelez le **3919** (gratuit, anonyme, 24 h sur 24) ou une association pour préparer ces étapes.
- Faites des **captures d'écran** des messages, des listes d'appareils et des applications suspectes avant de supprimer quoi que ce soit : ce sont des preuves.
- Si vous pensez que votre téléphone est surveillé, changez vos mots de passe depuis un appareil sûr : celui d'une personne de confiance ou un ordinateur public.
- En cas de danger : le **17**, ou le **114 par SMS** si vous ne pouvez pas parler.

1 Couper les partages de position

- [ ] **iPhone (iOS 16 ou plus) :** `Réglages › Confidentialité et sécurité › Contrôle de sécurité`. « Gérer les partages et les accès » permet de choisir personne par personne ; « Réinitialisation d'urgence » coupe tous les partages d'un coup. Le bouton « Quitter » ferme l'écran instantanément. Quand vous arrêtez de partager votre position dans Localiser, l'autre personne n'en est pas avertie.
- [ ] **Android :** dans Google Maps, touchez votre photo de profil, puis `Partage de position`, et retirez les personnes.
- [ ] **Applications :** la carte de Snapchat (mode Fantôme), Life360 et les autres applications familiales, les montres et traceurs partagés.
- [ ] **Traceurs cachés (sac, voiture) :** sur iPhone, `Localiser › Moi › Personnaliser les notifications de suivi`. Sur Android 12 ou plus, `Paramètres › Sécurité et urgence › Alertes de traceurs inconnus`, puis « Rechercher maintenant ».

2 Reprendre la main sur le téléphone

- [ ] Changez le **code de déverrouillage** pour un code que l'autre personne ne peut pas deviner : ni date d'anniversaire, ni code déjà utilisé.
- [ ] Supprimez les **visages et empreintes** ajoutés : sur iPhone, `Face ID et code › Réinitialiser Face ID`, ou supprimez les empreintes inconnues dans Touch ID. Sur Android, `Paramètres › Sécurité › Empreintes digitales`.
- [ ] Retirez les **appareils inconnus** de votre compte : sur iPhone, `Réglages › votre nom`, puis l'appareil, puis « Supprimer du compte ». Pour Google : `myaccount.google.com › Sécurité › Vos appareils`.
- [ ] Passez en revue les **applications** que vous ne reconnaissez pas, surtout celles qui ont accès à la position, au micro ou à l'administration de l'appareil.

3 Sécuriser les comptes, la boîte mail en premier

- [ ] **La boîte mail d'abord :** elle sert à réinitialiser tous les autres comptes. Nouveau mot de passe, puis vérifiez l'adresse et le numéro de secours, qui ne doivent pas être ceux de l'autre personne.
- [ ] **Ensuite :** le compte Apple ou Google, les réseaux sociaux, la banque, l'opérateur, puis impots.gouv.fr ou le compte qui vous sert à vous connecter avec FranceConnect (Ameli, CAF, retraite).
- [ ] Activez la **double authentification**, avec votre numéro de téléphone.
- [ ] **Déconnectez les sessions ouvertes :** WhatsApp, `Appareils connectés` ; Facebook et Messenger, « Où vous êtes connecté » ; Google, `Contrôle de sécurité` ; Instagram et Snapchat, dans les réglages de sécurité.
- [ ] Changez les **réponses aux questions secrètes** que l'autre personne connaît (nom du premier animal, ville de naissance).

4 Faire le tour de ce qui reste partagé

- [ ] **Photos et cloud**
  Albums partagés, Partage familial Apple, groupe familial Google : quittez le groupe ou retirez la personne.
- [ ] **Abonnements**
  Netflix, Amazon, Uber, livraison de repas, jeux : ils montrent souvent vos adresses et votre historique.
- [ ] **Maison et voiture**
  Voiture connectée, caméras, babyphone, box internet, serrure ou chauffage connectés : changez les mots de passe et retirez les utilisateurs.
- [ ] **Banque et enfants**
  Compte joint et accès à l'application : prévenez votre banque. Les appareils des enfants partagent parfois votre position : vérifiez leurs réglages aussi.

5 Si vous soupçonnez un logiciel espion

- [ ] **Les signes :** l'autre personne connaît des messages, des lieux ou des conversations que vous n'avez pas partagés ; la batterie se vide vite ; une application inconnue a beaucoup d'autorisations.
- [ ] **Ne le supprimez pas sans conseil :** la suppression prévient souvent la personne qui l'a installé et efface une preuve. L'association Echap, une association d'aide aux victimes ou la gendarmerie peuvent vous aider à l'analyser.

6 Qui contacter

3919
Violences Femmes Info : écoute et orientation, gratuit, anonyme, 24 h sur 24. Ce n'est pas un numéro d'urgence.

17 ou 112
En cas de danger immédiat. **114** par SMS ou avec l'application urgence114 si vous ne pouvez pas parler.

116 006
Aide aux victimes, tous les jours de 9 h à 20 h.

Echap
echap.eu.org : association spécialisée dans les technologies utilisées dans les violences.

Cybermalveillance.gouv.fr
Aide en cas de compte piraté.

Sources : Apple, guide Sécurité personnelle ; Google, aide Android sur les traceurs inconnus ; Service Public, violences conjugales (F12544) ; Centre Hubertine Auclert, guide Protéger sa vie privée sur son mobile ; Coalition Against Stalkerware.
Fiche réalisée par Alexis Valin, fondateur de Tout sur la cyber, formé à la cybersécurité par la SecNumacadémie de l'ANSSI. Libre de diffusion et d'impression. Version à jour sur toutsurlacyber.fr.