Fiche pratique

Version 2 · novembre 2026

Réglages de mon téléphone et de mes comptes

Les réglages à vérifier, à votre rythme.

Cochez chaque case au fur et à mesure. Vous pouvez faire ces étapes en plusieurs fois, ou avec une bénévole d'association.

Avant de commencer

- Couper un accès ou changer un mot de passe peut l'alerter. Si vous avez peur de sa réaction, appelez d'abord le **3919** : gratuit, anonyme, 24 h sur 24, et l'appel n'apparaît pas sur les factures de téléphone.
- Si votre téléphone est surveillé, ou si vous en doutez, lisez cette fiche et faites vos démarches depuis un **appareil sûr** : celui d'une personne de confiance, ou un ordinateur d'association ou de médiathèque.
- Gardez des **preuves hors de sa portée** : captures d'écran des messages, des listes d'appareils et des applications suspectes. Vérifiez d'abord que vos photos ne partent pas dans un album ou un cloud qu'il voit, puis rangez les preuves sur **Mémo de vie** (memo-devie.org, de France Victimes, avec un bouton « Vite je quitte ») ou remettez une copie à une personne sûre.
- En cas de danger : le **17** ou le **112**, ou le **114 par SMS** si vous ne pouvez pas parler.

La séparation se passe bien

Suivez les étapes 1 à 6 dans l'ordre, en une ou plusieurs fois.

Vous avez peur de sa réaction

Commencez par les preuves et le 3919, puis décidez avec une association de ce que vous coupez, et quand.

1 Votre ligne et vos comptes Apple ou Google

- [ ] Si le **forfait est à son nom**, il voit les factures et peut demander une nouvelle carte SIM. Ouvrez une ligne à votre nom, ou demandez à l'opérateur un changement de titulaire.
- [ ] Si votre téléphone utilise **son compte Apple ou Google**, il voit vos photos, vos sauvegardes et la position du téléphone. Créez un compte à votre nom, puis transférez vos données vers ce compte. S'il organise le **partage familial**, quittez le groupe.

2 Couper les partages de position

- [ ] Sur **iPhone** (iOS 16 ou plus), ouvrez `Réglages › Confidentialité et sécurité › Contrôle de sécurité`. « Gérer les partages et les accès » permet de choisir personne par personne, « Réinitialisation d'urgence » coupe tout d'un coup, et le bouton « Quitter » ferme l'écran instantanément. Quand vous arrêtez de partager votre position dans Localiser, l'autre personne n'en est pas avertie.
- [ ] Sur **Android**, dans Google Maps, touchez votre photo de profil, puis `Partage de position`, et retirez les personnes.
- [ ] Pensez aux **applications** : la carte de Snapchat (mode Fantôme), Life360 et les autres applications familiales, les montres et traceurs partagés.
- [ ] Cherchez les **traceurs cachés** dans un sac ou une 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 ».

3 Reprendre la main sur le téléphone

- [ ] Changez le **code de déverrouillage** pour un code qu'il 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 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.

4 Sécuriser les comptes, la boîte mail en premier

- [ ] Commencez par la **boîte mail**, qui sert à récupérer tous les autres comptes : nouveau mot de passe, puis une adresse et un numéro de secours qui sont les vôtres.
- [ ] Un changement de mot de passe ou d'adresse de secours peut envoyer une **alerte à l'ancienne adresse**. Si c'est la sienne, il sera prévenu : préparez ce moment avec une association.
- [ ] Continuez avec le compte Apple ou Google, les réseaux sociaux, la banque, l'opérateur, puis impots.gouv.fr et le compte FranceConnect (Ameli, CAF, retraite). Activez la **double authentification** avec votre numéro.
- [ ] **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 aussi les réponses aux questions secrètes qu'il connaît.

5 Faire le tour de ce qui reste partagé

- [ ] **Photos et cloud**
  Albums partagés, partage familial, 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**
  Un compte joint montre vos achats, donc les lieux où vous passez. Ouvrez un compte à votre seul nom, si possible dans une autre banque.
- [ ] **Les enfants**
  Un traceur glissé dans un sac ou un doudou, une montre ou une tablette offerte, un contrôle parental qu'il administre peuvent révéler où vous êtes. En garde alternée, retirer ces accès peut aller contre un accord : demandez d'abord conseil à une association ou à un avocat.

6 Si vous soupçonnez un logiciel espion

- [ ] Les signes qui alertent : il 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.

7 Vos droits et qui contacter

Suivre la position de quelqu'un sans son accord, lire ses messages ou installer un logiciel espion sur son téléphone sont des délits. Vos preuves servent pour une plainte ou pour demander une ordonnance de protection au juge aux affaires familiales. Vous pouvez aussi signaler les faits sur un **tchat gratuit et anonyme** avec la police ou la gendarmerie, 24 h sur 24 : arretonslesviolences.gouv.fr.

3919
Violences Femmes Info : écoute et orientation, gratuit, anonyme, 24 h sur 24, absent des factures. 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.

Mémo de vie
memo-devie.org : un espace sécurisé de France Victimes pour garder vos preuves et vos documents.

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

Cybermalveillance
cybermalveillance.gouv.fr : aide en cas de compte piraté.

Sources : Service Public, violences conjugales (F12544) ; Centre Hubertine Auclert, fiche Mémo de vie et guide Protéger sa vie privée sur son mobile ; Apple, guide Sécurité personnelle ; Google, aide Android sur les traceurs inconnus ; Code pénal, article 226-1 ; 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.