Checklist de sécurité Signal

ACTIVIST CHECKLIST

Dernière mise à jour le **3 avril 2026** Durée : environ **15 min**

Cette copie a été faite le 19 novembre 2026. On met souvent nos guides à jour, au fil de l'évolution des menaces et des nouvelles façons de se protéger. Pour la version la plus récente, rends-toi sur **activistchecklist.org/fr/signal/**

Traduction automatique: Cette page a été traduite automatiquement. Seuls 0 % de cette page ont été relus par des humains pour l'instant. Le reste peut contenir des erreurs. Aide-nous à relire cette traduction[1].

Ce guide t'aide à reprendre le contrôle de tes conversations privées sur Signal[2]. Signal chiffre déjà tout ce que tu envoies, mais ces étapes supplémentaires permettent de garder tes conversations privées, même si ton téléphone est perdu, saisi ou compromis. Tu vas découvrir des moyens simples de protéger tes messages, tes notifications et ton identité.

Tu débutes sur Signal ? Jette un œil à ce guide pour bien débuter avec Signal[3].

Astuce : configurer Signal, ça marche bien en session de groupe entre ami·es[4]. La plupart des étapes prennent 5 à 10 minutes une fois que tu t'y mets.

Cache ton identité sur Signal

TOUT LE MONDE Cette section s'adresse à toute personne qui milite ou fait du plaidoyer.

N'utilise pas ton vrai nom ni ta photo sur ton profil Signal

Ça t'aide à te protéger des flics ou des personnes malveillantes qui veulent te désanonymiser. Particulièrement utile si tu fais partie de groupes Signal non vérifiés.

Une grande partie de l'organisation militante se fait dans des groupes Signal non vérifiés, où tu ne sais pas à quel point tu peux faire confiance à tout le monde dans le groupe. Ces groupes peuvent être infiltrés par des adversaires d'extrême droite[5] et par les flics[6].

Utiliser un faux nom empêche quelqu'un de retrouver ta véritable identité avec une simple recherche Google.

Utiliser une photo qui n'est pas celle de ton visage empêche quelqu'un de retrouver tes profils sur les réseaux sociaux grâce à une correspondance d'image ou à la reconnaissance faciale.

Ces deux mesures t'aident à te protéger contre le doxxing[7] et le harcèlement en ligne.

COMMENT MODIFIER TON PROFIL

1. **Modifie le nom affiché sur ton profil :** Ouvre Signal → Touche ta photo de profil → **Paramètres** → Touche ton nom/ton icône en haut → Clique sur le premier élément avec la silhouette d'une personne → Modifie le nom affiché sur ton profil
2. **Modifie ta photo de profil :** Ouvre Signal → Touche ta photo de profil → **Paramètres** → Touche ton nom/ton icône en haut → **Modifier la photo** → importe une photo générique trouvée en ligne, sans lien avec ton identité/tes préférences/tes centres d'intérêt/ta localisation.

Le même principe s'applique encore plus aux réseaux sociaux. Si ton profil Instagram, Facebook ou LinkedIn associe ton vrai nom complet à une photo nette de ton visage, des personnes malveillantes peuvent facilement t'identifier, même si le reste de ton profil est privé. Pour en savoir plus, consulte Verrouille tes réseaux sociaux.

Rappelle aux personnes de tes groupes de faire la même chose. La sécurité, c'est un sport d'équipe.

Activer le nom d'utilisateur et masquer ton numéro de téléphone

Si tu veux pouvoir rester anonyme sur Signal, protéger ton numéro de téléphone aide à protéger ton identité.

Si tu as installé Signal avant mars 2024, quand les noms d'utilisateur[8] ont été introduits, ton numéro de téléphone est peut-être encore visible par les autres.

COMMENT ACTIVER LES NOMS D'UTILISATEUR ET MASQUER TON NUMÉRO DE TÉLÉPHONE

1. Assure-toi d'abord de changer ton nom de profil (voir l'élément ci-dessus). Si ton nom de profil Signal est ton nom complet, masquer ton numéro de téléphone ne t'aidera que très peu.
2. **Si tu veux changer ton nom d'utilisateur :** Ouvre Signal → Touche ta photo de profil → **Paramètres** → Touche ton nom/ton icône en haut → Touche le symbole **@** → **Modifier le nom d'utilisateur** → choisis un nom d'utilisateur **sans aucun rapport** avec ton identité ni avec les noms d'utilisateur que tu as déjà utilisés ailleurs. Il doit se terminer par au moins 2 chiffres.
3. **Masque ton numéro de téléphone :** Ouvre Signal → Touche ta photo de profil → **Paramètres** → **Confidentialité** → **Numéro de téléphone** → Sous **Qui peut voir mon numéro** → Sélectionne **Personne**.
    1. Si tu veux, tu peux aussi modifier « Qui peut me trouver grâce à mon numéro ». Mais du coup, aucun de tes contacts actuels ne saura que tu es déjà sur Signal, sauf si tu leur envoies un message en premier. Ne choisis « Personne » que si tu as besoin d'un niveau de confidentialité très élevé.
4. **Partage ton nom d'utilisateur plutôt que ton numéro de téléphone :** si tu entres en contact avec une nouvelle personne dans un cadre politique, partage ton nom d'utilisateur. Ouvre Signal → Touche ta photo de profil → **Paramètres** → Touche ton nom/ton icône en haut → **Code QR ou lien** → partage le code QR ou le lien avec la personne avec qui tu veux rester en contact. Ou plus simplement, donne-lui juste ton nom d'utilisateur.

Désactiver les aperçus de liens

Peut éviter que ta position approximative soit révélée

Ça te protège contre certaines attaques. Mais pense toujours à bien regarder l'URL qu'on t'envoie pour vérifier qu'elle vient d'un site que tu peux ouvrir en toute confiance.

COMMENT DÉSACTIVER LES APERÇUS DE LIENS

Ouvre Signal → Touche ta photo de profil → **Paramètres** → **Conversations** → **Désactive Générer les aperçus de liens**

Contexte technique : Une attaque a été publiée[9] en 2025. Elle permet à une personne malveillante d'estimer ta position à environ 250 miles près.

Active « Toujours relayer les appels »

Par défaut, les appels Signal se connectent directement entre toi et l'autre personne. Ça veut dire que l'appareil de l'autre personne peut voir ton adresse IP. Avec une décision de justice adressée à ton fournisseur d'accès à Internet, ton adresse IP peut servir à t'identifier personnellement.

Activer « Toujours relayer les appels » fait passer tes appels par les serveurs de Signal, ce qui cache ton adresse IP à l'autre personne. (Si tu utilises déjà un VPN[10], ton adresse IP est déjà masquée.)

COMMENT ACTIVER TOUJOURS RELAYER LES APPELS

Ouvre Signal → Touche ta photo de profil → **Paramètres** → **Confidentialité** → **Avancé** → Active **Toujours relayer les appels**

Protège tes messages et tes appels

TOUT LE MONDE Cette section s'adresse à toute personne qui milite ou fait du plaidoyer.

- [ ] Important **Modifie tes paramètres par défaut pour que les messages éphémères soient activés dans toutes tes nouvelles conversations Signal**

  Comme ça, tout le monde est mieux protégé si le téléphone de quelqu'un est un jour confisqué ou piraté.

La meilleure amélioration que tout le monde peut apporter à son utilisation de Signal, c'est de s'assurer que les messages éphémères[11] sont activés ***par défaut***. La plupart des militant·es avec qui on parle ne les ont pas activés par défaut. (Et la plupart des gens oublient de les activer manuellement pour chaque nouvelle conversation.)

Ça te protège, et ça protège les autres aussi. On ne sait jamais quel téléphone sera saisi par les flics. Même si on pense parler de choses parfaitement légales, le gouvernement peut trouver des moyens de déformer nos propos pour essayer de monter un dossier contre nous à cause de notre engagement politique

Il y a deux choses à surveiller avec les messages éphémères :

1. **D'abord, modifie ton paramètre par défaut** pour que cette fonctionnalité soit activée dans toutes les conversations que tu crées.
2. **Ensuite, vérifie qu'elle est activée dans les conversations lancées par d'autres personnes :** si quelqu'un d'autre lance la conversation, les messages éphémères ne sont peut-être pas activés. Tu devras peut-être les activer toi-même.

COMMENT ACTIVER LES MESSAGES ÉPHÉMÈRES

1. **Pour modifier le paramètre par défaut :** Ouvre Signal → Appuie sur ta photo de profil → **Paramètres** → **Confidentialité** → **Messages éphémères** → choisis la durée souhaitée (plus longue ou plus courte selon ta tolérance au risque).
2. **(Android uniquement) Modifie ta limite de conservation des messages :** ça supprimera les messages même dans les conversations où les messages éphémères ne sont pas activés. (Ils seront supprimés uniquement sur ton appareil.) Ouvre Signal → Appuie sur ta photo de profil → **Paramètres** → **Données et stockage** → **Gérer le stockage** → **Conserver les messages** → choisis la durée maximale souhaitée. Reviens à l'écran précédent et active **Appliquer les limites aux appareils associés**.
3. **Pour modifier les conversations existantes :** Signal → Ouvre la conversation à modifier → Appuie sur le nom de la personne (ou du groupe) en haut de l'écran → **Messages éphémères** → choisis la durée souhaitée.
4. **Supprime les anciens messages/conversations :** les messages éphémères ne s'appliquent PAS de manière rétroactive. Tu voudras donc peut-être supprimer les anciennes conversations sur ton téléphone. Malheureusement, ça ne les supprimera pas sur les téléphones des autres. Donc si c'est très sensible, tu devras peut-être leur demander de supprimer aussi la conversation manuellement. (Et tant que tu y es, encourage-les à activer les messages éphémères par défaut !)

Choisir la durée de tes messages éphémères : la durée que tu choisis dépend de la sensibilité de tes messages. Une question que tu peux te poser : si l'appareil de quelqu'un était confisqué ou piraté, à quel point est-ce important que ces messages ne soient pas accessibles ?

- Pour discuter de choses peu risquées entre ami·es, tu peux choisir 4 semaines.
- Pour l'organisation politique courante, tu peux choisir 1 semaine.
- Pour des actions plus risquées, tu peux régler la durée sur 1 jour, 1 heure ou 5 minutes, pour que les messages aient disparu avant le début de l'action.

Remarque : les messages ne disparaissent qu'une fois qu'ils ont été lus. Donc si la personne destinataire ne le lit qu'au bout de 2 semaines, et que tes messages éphémères sont réglés sur 4 semaines, il disparaîtra en réalité 6 semaines après son envoi.

Masquer l'aperçu des messages et le nom de l'expéditeur·rice dans les notifications Signal

Si ton téléphone est confisqué, les flics peuvent accéder à ton historique de notifications.

Si ton téléphone est confisqué, les flics ont deux moyens d'accéder à ton historique de notifications :

1. Ils peuvent voir les notifications sur ton écran d'accueil sans déverrouiller ton téléphone.
2. S'ils utilisent des outils de piratage, ils peuvent accéder au journal des notifications que ton téléphone a reçues. (Exemple tiré de l'affaire Prairieland[12].)

Ça ne concerne que les messages reçus. Et le risque existe même une fois que le message a disparu de Signal (si tu as activé les messages éphémères).

COMMENT DÉSACTIVER LES NOTIFICATIONS SIGNAL

SUR IPHONE

Ouvre Signal → Touche ta photo de profil → Paramètres → Notifications → Contenu des notifications → **Sélectionne « Ni nom ni contenu »**

SUR ANDROID

Ouvre Signal → Touche ta photo de profil pour ouvrir les Paramètres → Notifications → Afficher → **Sélectionne « Ni nom ni message »**

Si tu désactives les notifications Signal au niveau du système d'exploitation de ton téléphone, tu ne seras pas averti·e des appels Signal entrants.

Si tu utilises Signal Desktop, pense à y désactiver aussi les notifications.

Pour info : si tu veux effacer le journal des notifications qu'iOS a déjà enregistré, la seule façon de le faire est de réinitialiser ton téléphone aux paramètres d'usine et de le configurer comme un nouvel appareil — sans restaurer une sauvegarde, car les sauvegardes contiennent l'historique des notifications.

Active le « Verrouillage de l'écran » et « Masquer dans le sélecteur d'apps »

Si tu passes ton téléphone à quelqu'un, le Verrouillage de l'écran ajoute une couche de sécurité supplémentaire.

- **Verrouillage de l'écran :** si tu passes ton téléphone déverrouillé à quelqu'un, cette option l'oblige à déverrouiller de nouveau avec le visage, l'empreinte digitale ou le PIN avant d'ouvrir Signal.
- **Masquer dans le sélecteur d'apps :** cette option masque tes messages quand tu passes d'une app à l'autre.

COMMENT MASQUER L'ÉCRAN DANS LE SÉLECTEUR D'APPS

IPHONE

Ouvre Signal → Touche ta photo de profil → **Paramètres** → **Confidentialité** → Active **Verrouillage de l'écran**, puis active **Masquer l'écran dans le sélecteur d'apps**

ANDROID

Ouvre Signal → Touche ta photo de profil pour ouvrir les **Paramètres** → **Confidentialité** → Active **Verrouillage de l'écran**, puis active **Sécurité de l'écran**

Désactiver « Afficher les appels dans Récents » (iPhone uniquement)

Ça empêche les flics de voir ton historique d'appels Signal s'ils confisquent ton téléphone.

COMMENT DÉSACTIVER "AFFICHER LES APPELS DANS RÉCENTS"

Ce réglage n'existe que sur iPhone : Ouvre Signal → Touche ta photo de profil → **Réglages** → **Confidentialité** → **Appels** → Désactive **Afficher les appels dans Récents**

Quitte les groupes Signal qui pourraient mettre d'autres personnes en danger

Ça aide à protéger ton réseau si ton téléphone est confisqué.

Si les flics confisquent ton téléphone, l'un des plus gros risques, c'est d'exposer tout ton réseau. Même si les gens n'utilisent pas leur vrai nom sur leur compte Signal, il y a quand même un identifiant unique derrière chaque nom d'utilisateur Signal. Et les flics peuvent s'en servir pour recouper l'identité de quelqu'un sur plein d'appareils saisis.

Tu dois à la fois quitter ET supprimer le groupe :

- Si tu quittes seulement le groupe, les anciens messages restent sur ton téléphone, ainsi que l'historique des personnes qui étaient dans le groupe.
- Si tu supprimes seulement le groupe, les nouveaux messages continueront d'arriver et la conversation réapparaîtra.

COMMENT QUITTER ET SUPPRIMER UN GROUPE SIGNAL

1. **Prévois comment rejoindre les groupes après coup :** Quand tu vas dans une situation où tu risques d'être arrêté·e, fais une liste sur papier, chez toi ou dans un endroit sûr, de tous les groupes et des personnes à contacter qui pourront te réajouter une fois l'action ou le passage de frontière terminé.
2. **Pour quitter le groupe :** Signal → [Groupe] → Touche l'icône du groupe en haut → **Quitter le groupe**
   - Si tu es la seule personne admin, tu dois soit retirer tous les membres, soit désigner un·e autre admin.
3. **Pour supprimer le groupe de ton téléphone :** Signal → Écran principal → Balaie la conversation vers la gauche → **Supprimer**
   - Ça ne la supprimera pas pour les autres.

Conseils d'hygiène numérique :

- Programme un rappel récurrent pour faire le ménage dans tes conversations Signal tous les 3 mois.
- Pense bien à noter quels groupes tu quittes et à qui tu peux demander de te réajouter après l'action.

Remarque : Si tu trouves ce processus super pénible et fastidieux (parce qu'il l'est !), c'est une raison de plus d'utiliser un téléphone secondaire[13] pour les actions. Ce téléphone ne serait jamais que dans le ou les deux groupes nécessaires pour mener à bien l'action ce jour-là.

Activer le PIN Signal et le blocage de l'inscription

Te protège des attaques avancées où quelqu'un « vole » ton numéro de téléphone et l'enregistre sur Signal

Si une personne malveillante très déterminée arrive à trouver ton numéro de téléphone, elle peut essayer d'en prendre le contrôle avec une technique appelée « SIM Swapping » ou en appelant ton opérateur pour lancer une « portabilité » de ton numéro vers un nouvel opérateur. La personne pourrait alors utiliser ton numéro pour créer un compte Signal et commencer à recevoir les messages qui te sont destinés.

Ce sont des attaques avancées qui ne touchent pas la plupart des gens. Malgré tout, c'est facile de protéger ton compte Signal.

Tu peux te protéger en activant le **blocage de l'inscription** sur Signal. Ça empêche quelqu'un de pirater ton compte, même si cette personne vole ton numéro de téléphone. Personne ne pourra créer un nouveau compte Signal avec ton numéro tant que ton compte n'aura pas été inactif pendant 7 jours.

Si tu oublies ton PIN, tu devras attendre 7 jours avant de pouvoir créer un nouveau compte (et tes contacts ne seront pas récupérés). En savoir plus sur le PIN et le blocage de l'inscription[14].

COMMENT ACTIVER LE PIN SIGNAL ET LE BLOCAGE DE L'INSCRIPTION

Active le blocage de l'inscription : Ouvre Signal → Touche ta photo de profil → **Paramètres** → **Compte** → Active **Blocage de l'inscription**

Renforce ton PIN : Tu as dû définir un PIN Signal lors de la configuration. Si tu ne t'en souviens plus ou si tu veux utiliser un PIN plus robuste, voici comment faire :

1. **Génère un PIN robuste :** Pour une sécurité maximale, utilise un PIN de 8 ou 10 chiffres et assure-toi qu'il soit généré par ordinateur. Voici un générateur de PIN aléatoire[15] que tu peux utiliser.
2. **Définis un PIN Signal :** Ouvre Signal → Touche ta photo de profil → **Paramètres** → **Compte** → **Créer/Modifier le PIN** (si tu ne connais pas déjà ton PIN).
3. **Enregistre ton PIN ou active les rappels de PIN :** Si tu utilises régulièrement un gestionnaire de mots de passe[16], enregistre ton PIN dedans. Si tu penses que tu pourrais oublier où tu as enregistré ton PIN, laisse les « Rappels de PIN » activés.

☐ Activer un clavier privé pour Signal (Android uniquement)

Sur Android, le clavier par défaut peut enregistrer ce que tu tapes.

COMMENT T'ASSURER D'AVOIR UN CLAVIER PRIVÉ SUR ANDROID

Remarque : ceci concerne uniquement les téléphones Android. iPhone : les claviers sont déjà privés, sauf si tu as installé un clavier tiers.

OPTION 1 (plus facile) - Activer un clavier incognito
Ouvre Signal → Appuie sur ta photo de profil → **Paramètres** → **Confidentialité** → **Sécurité de l'application** → Active **Clavier incognito**

OPTION 2 (plus privée) - Remplacer le clavier intégré sur tout l'appareil

- L'option ci-dessus se contente de « demander » au fournisseur du clavier (Google) de ne pas enregistrer tes frappes. Rien ne garantit qu'il respecte cette demande. Le plus sûr, c'est d'installer un clavier tiers.
- FlorisBoard[17] est une bonne option. Tu dois d'abord installer F-Droid[18], un magasin d'applications plus respectueux de la vie privée.

☐ Désactiver les résumés de notifications par IA

Google et Apple ne disent pas clairement quand leurs outils d'IA envoient nos informations privées (comme nos messages Signal) depuis notre appareil vers leurs services. Si elles sont envoyées sur leurs serveurs, le gouvernement risque d'y accéder grâce à une décision de justice.

D'après ce qu'on comprend, ces fonctionnalités d'IA se contentent ***actuellement*** de résumer les notifications. Mais vu la tournure que prennent les choses, elles pourraient devenir plus intrusives.

Lis notre article Apple Intelligence lit-elle mes messages Signal ?[19]

OPTION A : COMMENT DÉSACTIVER LES RÉSUMÉS DE NOTIFICATIONS PAR IA UNIQUEMENT POUR SIGNAL

Option A : Désactiver les résumés de notifications par IA uniquement pour Signal

IPHONE

Ouvre l'app **Réglages** → **Notifications** → **Résumer les notifications** → Désactive **Signal**

ANDROID

Paramètres → **Notifications** → **Résumés des notifications** → **Gérer les applis** (sous **Ne pas inclure ces applis**) → Désactive **Signal**

COMMENT DÉSACTIVER COMPLÈTEMENT LES RÉSUMÉS DE NOTIFICATIONS PAR IA

Option B : Désactiver complètement les résumés de notifications par IA

IPHONE

Ouvre l'app **Réglages** → **Apple Intelligence et Siri** → Désactive **Apple Intelligence**

ANDROID

Ouvre **Paramètres** → **Notifications** → Désactive **Utiliser les résumés des notifications** (ou **Résumés des notifications**)

MAC

> **Réglages Système** → **Apple Intelligence et Siri** → Désactive **Apple Intelligence** → **Confirmer**

(Sur Mac, il faut un ordinateur Apple équipé d'un processeur M1 ou plus récent.)

Méfie-toi des faux messages du « Signal Support » qui essaient d'obtenir ton PIN Signal ou ton code de vérification

Protège ton compte en faisant attention à ne jamais donner ton code de vérification ou ton PIN

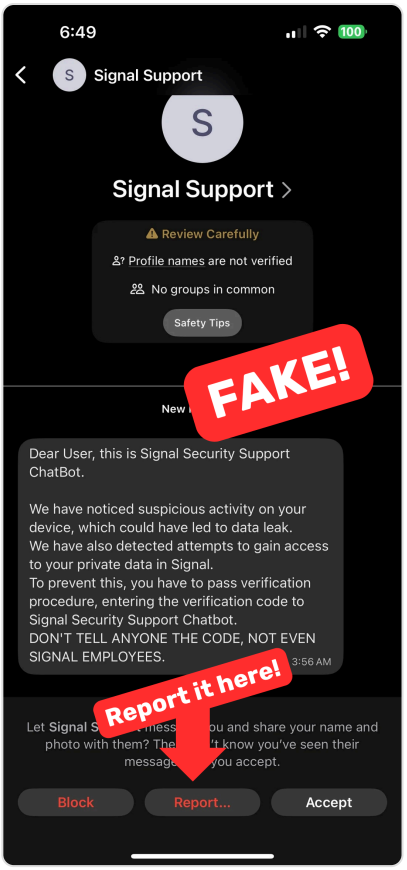
On voit de plus en plus de faux messages du « Signal Support »[20] qui tentent de pirater ton compte.

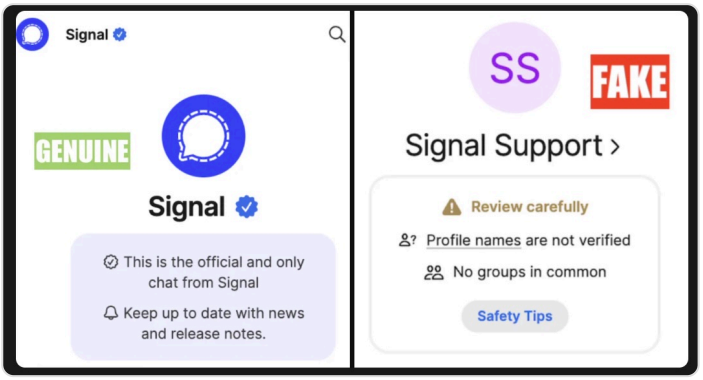
Sers-toi des exemples ci-dessous pour repérer les faux messages Signal.

Rappel : Signal ne te demandera jamais de lui envoyer ton PIN ou ton code de vérification. On te les demandera uniquement quand tu installes l'application pour la première fois sur un appareil.

En savoir plus sur les arnaques et le phishing sur Signal.[21]

Voici quelques exemples de messages frauduleux :





Sécurise ton téléphone

Signal n'est sécurisé que si le téléphone sur lequel il est installé l'est aussi. Si ton appareil est confisqué ou piraté, les flics disposent d'outils d'extraction forensique capables de casser les codes faibles et de récupérer tes messages directement sur ton appareil. Ces étapes protègent tes messages Signal au niveau de l'appareil.

TOUT LE MONDE Cette section s'adresse à toute personne qui milite ou fait du plaidoyer.

Choisis un code de 8 à 10 chiffres aléatoires pour ton téléphone

Il faut des années aux flics pour craquer un code aléatoire à 8 chiffres. Avec des outils automatisés, ils peuvent sans doute deviner ton code actuel en moins de 5 minutes.

DO: Utilise ton gestionnaire de mots de passe ou notre générateur de codes intégré pour créer un code aléatoire de 8 à 10 chiffres

DO NOT: Utiliser un code que tu as inventé toi-même (dates, motifs sur le clavier, etc.). Si possible, n'utilise pas de code à 6 chiffres.

COMMENT CHANGER TON CODE

1. **Choisis un code d'accès aléatoire de 8 à 10 chiffres.** Le moyen le plus sûr de générer un code aléatoire, c'est d'utiliser la fonction de génération de mots de passe aléatoires de ton gestionnaire de mots de passe (règle-la sur « chiffres uniquement »), mais tu peux aussi utiliser notre générateur de codes d'accès. (Les humains sont nuls pour inventer des codes aléatoires, donc on te conseille de ne pas essayer d'en trouver un toi-même.)
2. Change ton code :

   IPHONE

   Réglages → **Face ID et code** → **Modifier le code** → **Options de code** → **Code numérique personnalisé**

   ANDROID

   Paramètres → **Sécurité** → **Verrouillage de l'écran** → Saisis ton verrouillage actuel → **Code PIN/Mot de passe** → Saisis un code
3. **Entraîne-toi à taper ton nouveau code** au moins 10 fois de suite, dès maintenant, pour avoir plus de chances de t'en souvenir. (Désactiver le déverrouillage par reconnaissance faciale ou empreinte digitale t'obligera à saisir ton code chaque fois que tu ouvres ton téléphone.)
4. Écris ton nouveau code sur papier et garde-le en lieu sûr chez toi jusqu'à ce que tu l'aies mémorisé. Ensuite, détruis le papier au bout de 2 à 3 semaines. Programmer un rappel sur ton téléphone peut t'aider.

Pour plus de sécurité, utilise un chronomètre pour choisir tes chiffres au hasard

Utiliser un générateur de code en ligne comporte quelques petits risques. Si tu veux le niveau de sécurité le plus élevé, tu peux utiliser la fonction chronomètre de ton téléphone.

1. Lance le chronomètre et arrête-le sans regarder l'écran.
2. Note le dernier chiffre (les centièmes de seconde).
3. Recommence jusqu'à avoir 8 à 10 chiffres.

Combien de temps faut-il pour craquer un code ?

TYPE DE CODE	TEMPS NÉCESSAIRE POUR LE CRAQUER (EN MOYENNE)	EXEMPLE
Motif à 6 chiffres *facile à deviner*	**Moins de 24 heures** pour le craquer	*333666 (motif courant)* ou *051182 (motif de date pour le 5 nov. 1982)*
Code *aléatoire* à 6 chiffres	**200 jours** pour le craquer	*238253*
Code *aléatoire* à 8 chiffres	**Plus de 40 ans** pour le craquer	*34780026*

Remarque : ces durées ne s'appliquent qu'aux téléphones. Les ordinateurs se craquent beaucoup plus vite et ont besoin de mots de passe bien plus robustes.

Sources : les estimations du tableau ci-dessus se basent sur le nombre de tentatives par seconde réellement observé avec les outils de piratage forensique utilisés par les flics. Si tu as besoin de plus de sécurité, utilise un code à 10 chiffres : il te protégera même dans les pires scénarios de craquage possibles. Consulte les sources indiquées dans la FAQ sur les codes ici[22].

Garde ton téléphone (et ton ordinateur portable) à jour avec la dernière version du système d'exploitation

Ça te protège des hackers, des logiciels espions et des outils de piratage de téléphone qu'utilisent les flics.

DO: Installe les mises à jour dès qu'on te le propose

DO NOT: Appuyer sans cesse sur le bouton « Mettre à jour plus tard »

Chaque nouvelle mise à jour du système d'exploitation corrige des failles de sécurité. Chaque mise à jour que tu n'as pas installée allonge la liste des moyens dont disposent les flics pour pirater ton appareil. Imagine un grand bâtiment avec de plus en plus de portes laissées déverrouillées.

Si ton système d'exploitation n'est pas à jour, beaucoup des autres recommandations de ce guide ne protégeront pas tes données.

Commence par ton téléphone. Si tu fais quelque chose de plus risqué, assure-toi de mettre à jour tous tes appareils.

COMMENT FAIRE LES MISES À JOUR

Comme les mises à jour de sécurité sont super importantes, **on a conçu un outil pour te guider pas à pas**.

Vérifie les mises à jour de ton téléphone et de ton ordinateur →

COMMENT FAIRE LES MISES À JOUR MANUELLEMENT

Si tu préfères faire les mises à jour manuellement, voici comment faire pour chaque appareil :

Clique pour afficher les étapes manuelles

iPhone

1. **Vérifie que ton appareil est toujours pris en charge :** Vérifie si ton iPhone est toujours pris en charge[23]
2. **Système d'exploitation :** **Réglages** → **Général** → **Mise à jour logicielle**
3. Les **apps** sont configurées par défaut pour se mettre à jour automatiquement. Pour vérifier, va dans **Réglages** → **Apps** → **App Store** et assure-toi que **Mises à jour des apps** est activé.

Mac

1. **Vérifie que ton appareil est toujours pris en charge :** Vérifie si ton Mac est toujours pris en charge[23]
2. **Système d'exploitation :** **Menu Pomme** → **Réglages Système** → **Général** → **Mise à jour de logiciels**
3. **Apps installées via le Mac App Store :** Ces apps sont configurées par défaut pour se mettre à jour automatiquement. Pour vérifier, ouvre l'**App Store**, va dans **App Store** → **Réglages** et assure-toi que **Mises à jour automatiques** est activé.
4. **Autres applications :** Recherche les mises à jour en allant dans barre des menus en haut → Clique sur le nom de l'application → Clique sur **Rechercher les mises à jour** ou **À propos de** [**NOM DE L'APP**], ou regarde dans **Réglages...**. Si tu ne vois pas d'option de mise à jour, il est possible que la mise à jour automatique en arrière-plan soit activée.

Android

1. **Vérifie que ton appareil est toujours pris en charge :** Vérifie si ton Android est toujours pris en charge[23]
2. **Système d'exploitation :** **Paramètres** → **Système** → **Mise à jour du système** (peut varier selon le fabricant)
3. Les **applications** du Google Play Store sont configurées par défaut pour se mettre à jour automatiquement. Pour vérifier, ouvre le **Play Store**, appuie sur l'icône de ton profil, puis va dans **Paramètres** → **Préférences réseau** → **Mise à jour automatique des applis**.

Windows

1. **Mets à jour ton système :** **Démarrer** → **Paramètres** → **Mise à jour et sécurité** → **Windows Update**
2. **Vérifie que ton appareil est toujours pris en charge :** Vérifie si ton ordinateur Windows est toujours pris en charge[23]
3. **Applications du Microsoft Store :** Assure-toi d'activer les mises à jour automatiques[24] (activées par défaut).
4. **Autres applications :** Cherche les mises à jour dans barre des menus → **Aide** → **Rechercher des mises à jour**, ou cherche **Mises à jour** ou **À propos** dans les paramètres de l'application.

Désactiver le déverrouillage par visage/empreinte (biométrique)

Tu es mieux protégé·e juridiquement[25] avec un code qu'avec le déverrouillage biométrique. Les flics peuvent essayer de te forcer à déverrouiller ton téléphone avec la biométrie.

COMMENT DÉSACTIVER LE DÉVERROUILLAGE PAR VISAGE/EMPREINTE

IPHONE

Réglages → **Face ID et code** → Désactive **Déverrouillage de l'iPhone** sous **Utiliser Face ID pour**

(Tu peux laisser le reste activé.)

ANDROID

Paramètres → **Écran de verrouillage** (ou **Sécurité**) → **Biométrie et sécurité** → **Désactive à la fois la Reconnaissance faciale et les Empreintes digitales** pour déverrouiller ton téléphone

Attention : le déverrouillage par visage ou par empreinte te permet d'utiliser des mots de passe plus solides sans avoir à les taper tout le temps. Si tu dois choisir, mieux vaut avoir un code plus long que désactiver le déverrouillage par visage/empreinte. Si tu laisses la biométrie activée, assure-toi de savoir la désactiver rapidement si tu t'apprêtes à te retrouver dans une situation à haut risque (voir les astuces ci-dessous).

Éteindre complètement ton téléphone, c'est la meilleure façon de désactiver temporairement la biométrie, parce que ça chiffre aussi tes données. Le prochain déverrouillage demandera ton code.

Astuce de verrouillage sur iPhone : si tu laisses le déverrouillage par visage/empreinte activé, tu peux forcer l'utilisation de ton code au prochain déverrouillage en **appuyant 5 fois sur le bouton latéral**.

Astuce appareil photo sur iPhone : tu peux prendre des photos sans déverrouiller ton téléphone en **balayant vers la gauche** sur ton écran d'accueil. (Au cas où tu te ferais arrêter en train de filmer.)

Astuce appareil photo sur Android : sur beaucoup de téléphones Android, tu peux lancer l'appareil photo sans déverrouiller en **appuyant deux fois sur le bouton latéral/marche-arrêt**.

Protection renforcée

RISQUE MOYEN

Cette section est pour toi si tu occupes un rôle de leader ou si ton militantisme a plus de chances d'être ciblé par l'État ou par tes adversaires.

Active le mode Isolement (iPhone) ou la Protection avancée (Google et Android)

Les logiciels espions sont un type d'attaque avancé, qui exploite des failles sophistiquées de nos appareils. Pour y répondre, Apple et Google ont introduit un mode de sécurité avancé qui offre une protection renforcée contre les logiciels espions.

Sur iPhone, ça s'appelle le **mode Isolement**[26] et sur Android, le **Programme Protection Avancée**[27]. (Tu peux aussi activer le Programme Protection Avancée uniquement sur ton compte Google, même si tu n'as pas de téléphone Android.)

Nous n'avons **aucun signalement** de personne infectée par un logiciel espion alors que le mode Isolement d'Apple était activé. La Protection avancée d'Android est plus récente et son efficacité reste encore à prouver.

Compromis d'utilisation : ces deux fonctionnalités impliquent de renoncer à certaines fonctions. Voir la liste complète des compromis[28]. Si tu rencontres des problèmes qui ne te conviennent pas, tu pourras toujours désactiver la fonctionnalité plus tard.

COMMENT ACTIVER LE MODE ISOLEMENT SUR IPHONE

IPHONE

Réglages → **Confidentialité et sécurité** → **Mode Isolement** → **Activer**

Cette fonctionnalité est disponible à partir d'iOS 16.

COMMENT ACTIVER LA PROTECTION AVANCÉE SUR ANDROID

ANDROID

Paramètres → **Sécurité et confidentialité** → sous **Autres paramètres**, appuie sur **Protection avancée**

Remarque : l'emplacement de ce réglage peut varier selon les appareils Android, alors on te conseille de rechercher « Protection avancée » dans la barre de recherche des Paramètres.

Cette fonctionnalité est disponible à partir d'Android 16.

Vérifie les numéros de sécurité avec tes contacts importants

Confirme que personne n'intercepte secrètement tes messages entre toi et l'autre personne

Signal chiffre tes messages pour que seules toi et l'autre personne puissiez les lire. Mais en théorie, un attaquant sophistiqué pourrait se placer entre toi et ton contact, et intercepter les messages avant de les faire suivre. C'est ce qu'on appelle une attaque de l'"homme du milieu". Les **numéros de sécurité** te permettent de confirmer que ta connexion chiffrée va directement à ton contact, sans personne au milieu.

La plupart des gens n'ont pas besoin de faire ça. Si tu discutes avec des ami·es d'organisation au quotidien, le chiffrement de Signal fait déjà son travail. Mais si tu communiques sur un sujet à haut risque (actions directes, affaires juridiques sensibles, journaliste qui échange avec une source), vérifier les numéros de sécurité vaut bien cette étape supplémentaire.

Imagine un sceau de cire sur une enveloppe. Le chiffrement, c'est le sceau, mais un attaquant sophistiqué pourrait le briser, lire le contenu, puis refermer l'enveloppe avec sa propre cire. Vérifier les numéros de sécurité, c'est s'assurer que personne n'a remplacé le sceau.

COMMENT VÉRIFIER LES NUMÉROS DE SÉCURITÉ

1. **Ouvre la conversation** avec la personne que tu veux vérifier → **Appuie sur son nom** en haut → **Afficher le numéro de sécurité**.
2. **Compare les numéros avec ton contact :**
   - **En personne (le mieux) :** Appuie sur "Scanner le code" et scanne son code QR. S'ils correspondent, tu verras un message de confirmation.
   - **À distance :** Lisez-vous les numéros lors d'un appel ou d'un appel vidéo où tu es sûr·e de parler à la bonne personne. Ne fais pas la vérification via Signal lui-même.
3. **Marque comme vérifié :** Si les numéros correspondent, appuie sur la coche.

Tu n'as besoin de faire ça qu'une seule fois par contact, sauf si ses numéros de sécurité changent (par exemple, s'il ou elle change de téléphone). Si ça arrive, Signal te préviendra. Refais la vérification avant de partager quoi que ce soit de sensible.

Signal a-t-il été piraté ? Est-ce sûr ? Est-ce sécurisé ?

Tous les quelques mois, on voit circuler des posts affirmant que Signal n'est pas sécurisé ou qu'il a été piraté.

Signal a-t-il été piraté ? Très probablement pas[29].

Pour une explication plus complète sur la sécurité de Signal, y compris son statut d'organisation à but non lucratif, le chiffrement, l'open source, les rumeurs sur son financement et les risques liés aux appareils, lis notre article : Signal est-il sécurisé ?[30].

Utiliser Signal comporte des risques, mais ils sont généralement liés à la façon de l'utiliser de manière sécurisée, plutôt qu'à la technologie elle-même.

Par exemple, si quelqu'un infiltre un groupe Signal privé, cette personne pourrait faire des captures d'écran de tous les messages et les publier en ligne.

Il est aussi possible que les flics confisquent ton téléphone et parviennent à y accéder si ton code de déverrouillage est faible. Mais ce n'est pas une faille de Signal. Tous tes messages sont accessibles à quiconque a physiquement accès à ton téléphone et peut le déverrouiller. C'est pour ça qu'on recommande d'avoir un code de déverrouillage solide[16] et de toujours mettre à jour le système d'exploitation de ton appareil[16].

Autres ressources

- Signal est-il sécurisé ?[30] — comment fonctionne Signal, quelles données il peut partager et les mythes courants sur sa sécurité.
- Voici un excellent guide sur comment utiliser les groupes Signal pour le militantisme[31].
- Verrouiller Signal[32] — Freedom of the Press Foundation

Continue d'apprendre avec ces guides

Les bases de la sécurité

Les essentiels que tout le monde devrait faire pour se protéger de la surveillance et des attaques.

Se préparer pour une manif

Pour toutes les personnes qui vont en manif.

Sécurité en voyage et en avion

Checklist pour les vols intérieurs comme internationaux. S'applique aussi aux passages de frontière par voie terrestre ou maritime.

Se protéger des logiciels espions

Protège-toi des logiciels espions et des logiciels de surveillance.

Les VPN pour militant·es 16 min de lecture 10 | Vérificateur de mises à jour de sécurité 23

Comment utiliser Proton en toute sécurité 17 min de lecture 33 | Supprimer le pistage des liens 3 min de lecture 34

Apple Intelligence lit-elle mes messages Signal ? 5 min de lecture 19

Liens

1. activistchecklist.org/fr/contribute/
2. signal.org
3. ssd.eff.org/module/how-to-use-signal
4. activistchecklist.org/fr/party/
5. nitter.net/camhigby/status/2015093531526729789
6. theguardian.com/us-news/2025/nov/21/fbi-signal-group-chat-immigration
7. activistchecklist.org/fr/doxxing/
8. signal.org/blog/phone-number-privacy-usernames/
9. gist.github.com/hackermondev/45a3cdfa52246f1d1201c1e8cdef6117
10. activistchecklist.org/fr/vpn/
11. support.signal.org/hc/en-us/articles/360007320771-Set-and-manage-disappearing-messages
12. bsky.app/profile/activistchecklist.org/post/3mityctmsfc2v
13. activistchecklist.org/fr/secondary/
14. support.signal.org/hc/en-us/articles/360007059792-Signal-PIN
15. activistchecklist.org/fr/passcode/
16. activistchecklist.org/fr/essentials/
17. florisboard.org
18. f-droid.org/en/
19. activistchecklist.org/fr/signal-ai/

20. netzpolitik.org/2026/phishing-attack-numerous-journalists-targeted-in-attack-via-signal-messenger/
21. support.signal.org/hc/en-us/articles/9932566320410-Staying-Safe-from-Phishing-Scams-and-Impersonation
22. strongphrase.net/passcode
23. activistchecklist.org/fr/updates/
24. support.microsoft.com/en-us/windows/turn-on-automatic-app-updates-70634d32-4657-dc76-632b-66048978e51b
25. ssd.eff.org/module/attending-protest
26. support.apple.com/en-us/105120
27. landing.google.com/intl/en_us/advancedprotection/
28. activistchecklist.org/fr/lockdown/
29. hassignalbeenhacked.info
30. activistchecklist.org/fr/signal-secure/
31. micahflee.com/using-signal-groups-for-activism/
32. freedom.press/digisec/blog/locking-down-signal/
33. activistchecklist.org/fr/proton/
34. activistchecklist.org/fr/links/