Sécurité numérique pour les actions à risque d'arrestation

ACTIVIST CHECKLIST

Dernière mise à jour le **30 octobre 2026** Durée : environ **20 minutes**

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/action/**

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 porte sur la sécurité numérique si tu dois emporter ton téléphone lors d'une action non violente de désobéissance civile (ou action directe) où certaines personnes prévoient de risquer l'arrestation. C'est un des éléments pour assurer la sécurité de ton groupe. Ton action doit aussi prévoir la sécurité physique, avoir une équipe de sécurité et s'assurer que tout le monde connaît ses droits. Notre checklist de sécurité pour les personnes qui organisent des actions[2] peut t'aider sur tous ces points.

Évalue ton niveau de risque : ce guide concerne les actions où tu prends un risque juridique relativement faible (par exemple : un sit-in ou t'enchaîner à une porte). Si tu prévois quelque chose où tu cherches à rester anonyme, ou où les conséquences juridiques sont beaucoup plus lourdes, tu dois prendre bien plus de précautions que ce que propose ce guide.

Ce guide a été écrit pour la situation suivante :

- L'action est suffisamment organisée de manière centralisée pour que vous puissiez établir des accords sur la sécurité numérique que tout le monde respectera.
- Tu as encouragé la plupart des personnes qui participent à l'action à **ne pas apporter leur téléphone**
- Certaines personnes ont quand même besoin de leur téléphone pour coordonner votre déploiement (par ex. : responsable tactique, medics, équipe de désescalade, etc.)
- Le risque d'arrestation est élevé, ou tu prévois de risquer l'arrestation.
- Tu penses que les flics pourraient essayer d'utiliser des outils pour craquer les téléphones afin d'accéder aux données des téléphones qu'ils confisquent.
- La surveillance sur le trajet aller et retour de l'action ne vous préoccupe pas.

Si l'un de ces points ne s'applique pas à ton action, tu devras peut-être prendre plus de précautions. Jette un œil à la section sur la sécurité renforcée du téléphone en manif[3] ou pense à emporter un téléphone secondaire[4] (parfois appelé « téléphone jetable »).

Conseil pour les organisateur·ices : en amont de l'action, pense à organiser une soirée sécurité[5] pour que ton équipe passe ces étapes ensemble avant le jour J.

Pourquoi c'est important ?

On sait que les mouvements sociaux sont surveillés, infiltrés, discrédités et entravés par des agents du gouvernement (flics locaux, FBI, CIA, NSA, etc.) depuis des décennies. Avec l'essor de la technologie, on est toutes et tous pisté·es et profilé·es (même si tu n'as jamais été arrêté·e).

Même quand on exerce nos droits légaux à la liberté d'expression et de réunion, de nombreuses forces gouvernementales cherchent à écraser la contestation et à criminaliser les militant·es. (Voir l'affaire des « Minnesota 15 »[6])

Mais on peut agir pour protéger nos mouvements ! Ce guide propose des gestes simples que nous pouvons toutes et tous faire avant et pendant une manif/action pour mieux protéger nos camarades, et surtout les personnes les plus exposées de nos mouvements. Prendre ces précautions aide à protéger toutes les personnes avec qui tu t'organises (pas seulement toi et

tes données). Ce n'est ni un signe ni un aveu d'avoir fait quoi que ce soit de mal.

Menaces à prendre en compte

- **Saisie et fouille du téléphone** - En cas d'arrestation, les flics peuvent essayer de pénétrer dans ton téléphone pour accéder à tes messages, photos et autres informations privées afin de les utiliser comme preuves
- **Surveillance des communications** - Les flics peuvent intercepter les SMS et appels classiques pour recueillir des infos sur les plans de la manif et les participant·es
- **Subpoena de les données de ton compte ou de ton opérateur mobile** - Les flics peuvent obtenir une décision de justice pour accéder à tes comptes en ligne (comme Google ou Apple) ou à tes données de communication et de localisation auprès de ton opérateur mobile.
- **Indics et agent·es infiltré·es** - Des personnes présentes dans tes réunions ou tes groupes de discussion peuvent transmettre aux flics ce qu'elles voient et lisent
- **Cartographie des réseaux militants** - En récupérant les données du téléphone d'une seule personne, les flics peuvent identifier des communautés entières de militant·es et d'organisateur·ices qui y sont lié·es

---

Pour toutes les personnes qui participent à l'action

☐ Important **Mettez-vous d'accord en groupe : toute personne qui risque l'arrestation confie son téléphone à une personne de soutien (ou le laisse à la maison)**

Des téléphones éteints et moins exposés au risque de saisie, c'est plus de sécurité pour tout le monde.

Pour les actions où le risque d'arrestation est plus faible, le mieux, c'est que tout le monde A) laisse son téléphone à la maison ou B) **éteigne son téléphone** et le confie à une personne de soutien. Souvent, c'est une personne qui fait du soutien aux personnes arrêtées. Cette personne ne devrait pas participer à l'action, ou alors rester à un poste à très faible risque, bien en périphérie de l'action.

COMMENT METTRE EN PLACE UN ACCORD SUR LES TÉLÉPHONES POUR VOTRE ACTION

1. **Décidez quels rôles ont vraiment besoin d'un téléphone.** En général, ça ne concerne que quelques personnes, comme la personne responsable tactique, la personne chargée du lien avec les flics ou les medics. Tout le monde laisse son téléphone à la personne de soutien. Les personnes qui ont un rôle à fort risque d'arrestation ne devraient pas apporter de téléphone. (Ou alors, elles devraient le remettre immédiatement après le déploiement.)
2. **Avant le déploiement, la personne de soutien récupère la plupart des téléphones.**
3. **Prévoyez comment rendre les téléphones aux gens après leur libération**. En général, c'est la personne chargée du soutien aux personnes arrêtées, le jail support, qui rapporte les téléphones aux gens après leur libération.
4. **Partagez l'accord tôt et répétez-le** pendant les formations et le briefing de l'action.

Astuce : s'il y a beaucoup de téléphones et que vous devez vérifier que chaque personne est bien la propriétaire du téléphone qu'elle désigne dans la pile, vous pouvez lui demander de le déverrouiller devant vous.

☐ **Utilise Signal pour communiquer (messages/appels) lors des manifs/actions**

Les messages chiffrés de bout en bout protègent ta vie privée contre la surveillance, alors que les SMS classiques peuvent être interceptés et lus.

DO: Installe et utilise l'application Signal[7] (gratuite) pour ton activisme/travail politique

DO NOT: Utiliser WhatsApp, Telegram, iMessage ou les SMS classiques (pour ton activisme)

COMMENT INSTALLER ET UTILISER SIGNAL

1. Installe Signal[8] sur ton téléphone
2. Envoie un message ou appelle tes contacts avec leur numéro de téléphone, ou demande à quelqu'un son nom d'utilisateur Signal. Ces personnes doivent aussi avoir installé Signal.

Consulte notre Checklist Signal[9] pour des instructions détaillées sur la configuration de Signal afin de le rendre le plus sécurisé possible.

- [ ] 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[10] 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.

Utilise Proton Docs pour collaborer (au lieu de Google Docs)

Protège les données de ton groupe : Google traque chaque doc que tu consultes

DO: Utilise Proton Docs (ou CryptPad) pour vous organiser

DO NOT: Utiliser Google Docs pour s'organiser

Google traque toute l'activité de ses utilisateur·ices, y compris les documents que tu ouvres, partages et consultes. Les flics peuvent obtenir ces données grâce à des mandats ou des assignations, et on sait qu'il leur est déjà arrivé de les partager sans autorisation en bonne et due forme. Nous organiser en dehors de Google Docs nous aide à mieux nous protéger les un·es les autres.

Proton Docs[11] est une alternative de qualité à Google Docs. Tes documents sont chiffrés de bout en bout : même si les autorités accédaient aux serveurs de Proton, elles ne pourraient pas voir ce qu'ils contiennent.

> **Proton Docs ne te rend pas anonyme par défaut !** Si tu t'organises dans un contexte plus risqué, prends le temps de comprendre les limites de Proton et comment l'utiliser en sécurité[12].

COMMENT UTILISER PROTON DOCS

1. Crée un compte Proton[13] si tu n'en as pas encore — choisis l'offre gratuite
2. Va sur Proton Drive[14] → Clique sur le bouton **Nouveau** → Sélectionne **Nouveau document**
3. Quand ton document est prêt à être partagé, clique sur le bouton « Partager » et partage-le avec d'autres comptes Proton, ou active « Créer un lien public » pour le partager avec des personnes qui n'ont pas de compte Proton. Fais attention à l'endroit où tu partages le lien, car il sera moins sécurisé ! On te conseille d'ajouter un mot de passe si tu actives le mode « Toute personne disposant du lien peut consulter ».

Encourage les personnes avec qui tu t'organises à se créer un compte Proton : comme ça, vous pourrez toustes avancer ensemble vers plus de sécurité.

Tu cherches des formulaires ? Proton n'a pas d'équivalent à Google Forms. Tu peux essayer les formulaires CryptPad[15] ou Jotform[16] en activant l'option de chiffrement de bout en bout.

N'écris rien que tu n'aimerais pas entendre lu à voix haute au tribunal

Les chats, les docs et les notes peuvent finir entre les mains des flics.

DO: Discute des détails sensibles en personne, téléphones rangés

DO NOT: Mettre qui risque l'arrestation, ou les détails du plan, dans des chats de groupe ou des docs partagés

On vit une époque où le gouvernement fédéral surveille et poursuit les militant·es avec une intensité qu'on n'avait pas vue depuis des décennies.

Quand on s'organise à grande échelle, on doit toujours trouver un équilibre entre le besoin de sécurité et le besoin de faire grandir nos mouvements et de construire du pouvoir.

Une façon de réduire les risques inutiles, c'est de faire attention à ce qu'on met par écrit. Ce qu'on écrit finit souvent par être utilisé contre nous au tribunal, même quand on utilise des outils chiffrés comme Signal.

Pour toute action qui implique un risque d'arrestation (ou une organisation particulièrement ciblée, comme l'ICE watch[17] ou la solidarité avec la Palestine), il est important de se mettre d'accord sur ce que personne ne mettra par écrit.

Comment les données finissent au tribunal :

- **Le téléphone de quelqu'un est saisi.** Si une personne du chat est arrêtée et que les flics accèdent à son téléphone, ils peuvent lire tous les messages et documents qui s'y trouvent.
- **Une entreprise livre ton compte.** Les services comme Google Docs ne sont pas chiffrés de bout en bout, donc l'entreprise peut voir tes documents et les donner aux flics qui ont obtenu une assignation ou un mandat. En 2025, Google a transmis à l'ICE les informations du compte d'un·e étudiant·e en master en réponse à une assignation dite « subpoena », sans l'en informer au préalable[18].
- **Quelqu'un dans le groupe est un·e indic ou un·e flic infiltré·e.** Dans l'affaire fédérale de 2026 contre les « Minnesota 15 », des agents infiltrés ont rejoint les chats de groupe Signal des militant·es[6] et ont transmis ce qu'ils y lisaient, que les procureurs ont ensuite utilisé au tribunal.

COMMENT GARDER TES PLANS HORS DE TOUTE TRACE ÉCRITE

Évite de mettre par écrit les choses les plus risquées, que ce soit dans des messages, des documents ou même des notes sur papier.

Avant de taper ou d'écrire quelque chose, demande-toi : « Est-ce que ça m'irait d'entendre ça lu à voix haute dans un procès contre moi ? » Si ce n'est pas le cas, garde-le pour une conversation en personne (idéalement avec tous les téléphones et appareils dans une autre pièce).

Ce que tu préféreras peut-être ne pas mettre par écrit :

- Le fait que tu prévois de faire quelque chose qui comporte un risque d'arrestation (même un sit-in très tranquille enfreint généralement une loi sur l'intrusion)
- Qui participe au groupe ou à l'action
- Qui mène
- Pour les actions : le lieu, les tactiques, les informations permettant d'identifier les personnes impliquées
- Les autres groupes impliqués
- Les blagues, coups de gueule ou sarcasmes qui pourraient être lus comme une menace ou une intention sérieuse.

Dernière étape : prends l'habitude de **supprimer/détruire ce que tu as mis par écrit dès que tu n'en as plus besoin**. On a tendance à l'oublier, alors mettre en place des systèmes pour se tenir mutuellement responsables peut aider.

Partez du principe que les grands groupes ou les groupes ouverts contiennent un·e informateur·ice. En général, c'est impossible de savoir qui en est un·e. Et c'est une mauvaise idée de se mettre à « chercher la balance » dans un groupe. Plus un groupe compte de monde, plus c'est difficile de connaître tout le monde. Réservez les conversations les plus sensibles à de petits groupes de personnes que vous connaissez et en qui vous avez confiance.

Choisis un numéro de téléphone que tu appelleras si tu te fais arrêter. Écris-le sur ton corps au marqueur indélébile.

C'est le numéro que tu appelleras si tu te fais arrêter, pour joindre quelqu'un qui peut te soutenir depuis l'extérieur. C'est important dans les situations à risque élevé.

COMMENT CHOISIR UN NUMÉRO DE TÉLÉPHONE À APPELER SI TU TE FAIS ARRÊTER

1. **Décide qui appeler si tu te fais arrêter :**
   - Si tu ne sais pas s'il existe une ligne d'urgence de soutien aux personnes arrêtées active dans ta région, choisis quelqu'un comme contact d'urgence et utilise son numéro de téléphone. Ça peut être un·e ami·e ou un·e camarade de confiance qui peut t'aider à obtenir un soutien juridique. Assure-toi d'avoir son accord à l'avance.
   - Si tu participes à une action à risque élevé, les organisateur·ices ont peut-être déjà mis en place un numéro de ligne d'urgence juridique spécifique à utiliser.
   - Si tu es dans une grande ville, il existe peut-être une ligne d'urgence de soutien aux personnes arrêtées du National Lawyers Guild, tenue par des personnes chargées de soutenir les militant·es. Consulte la liste des numéros de lignes d'urgence de soutien aux personnes arrêtées du NLG ici[19]. On recommande d'utiliser une ligne d'urgence seulement si tu as rempli un formulaire de soutien aux personnes arrêtées à l'avance, pour qu'elle puisse appeler tes contacts à ta place tout en t'apportant du soutien.
2. **Écris le numéro de la ligne d'urgence juridique sur ton corps au marqueur indélébile** à un endroit où il ne peut pas facilement s'effacer (haut du bras, jambe, torse). Appelle ce numéro si tu te fais arrêter et qu'on te laisse passer un coup de fil.

Verrouiller son téléphone (pour toutes les personnes qui apportent un téléphone)

Si tu fais partie des personnes qui apportent un téléphone et que tu as des données très sensibles sur ton téléphone principal, ou que tu risques fortement d'être ciblé·e par les flics, on te recommande de suivre toutes les étapes de ce guide avec un téléphone secondaire[4] qui contiendra moins de données.

- [ ] **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[20]
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[20]
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[20]
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[20]
3. **Applications du Microsoft Store :** Assure-toi d'activer les mises à jour automatiques[21] (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.

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].

Désactiver le déverrouillage par visage/empreinte (biométrique)

Tu es mieux protégé·e juridiquement[23] 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**.

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[4] 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.

Pendant l'action (si tu as apporté un téléphone)

☐ Important Éteins complètement ton téléphone si ton risque d'arrestation augmente

Tes données sont mieux protégées quand ton téléphone est éteint (pas seulement verrouillé)

Quand ton téléphone est complètement éteint, il est mieux protégé contre l'extraction de données par les flics. Les données restent chiffrées jusqu'à ce que tu saisisses ton code d'accès pour la première fois.

Donc, la chose la plus importante que tu puisses faire pour protéger tes données, c'est d'éteindre ton téléphone dès que tu penses que ton risque d'arrestation augmente.

COMMENT ÉTEINDRE TON TÉLÉPHONE

1. IPHONE
   Appuie **5 fois** sur le bouton de verrouillage sur le côté pour afficher rapidement l'option **Éteindre**

   ANDROID
   Maintiens le bouton d'alimentation enfoncé jusqu'à ce que le menu d'alimentation s'affiche → appuie sur **Éteindre**
2. **Entraîne-toi** plusieurs fois pour pouvoir le faire rapidement.
3. Pendant une situation à haut risque, **rappelle aux personnes autour de toi** d'éteindre aussi leur téléphone.

Compromis : On sait bien qu'éteindre son téléphone implique des compromis. Parfois, c'est plus important de filmer les flics ou de se coordonner avec nos allié·es. Réfléchis à ce qui est prioritaire pour toi. Si tu as besoin de filmer, pense à emporter un téléphone secondaire[4] pour avoir moins de données sensibles sur toi.

☐ Confie ton téléphone à quelqu'un qui ne risque pas l'arrestation

Ne pas avoir ton téléphone sur toi quand tu es placé·e en garde à vue, c'est le meilleur moyen de protéger tes données et le mouvement. L'éteindre complètement, c'est la deuxième meilleure option.

COMMENT CONFIER TON TÉLÉPHONE À QUELQU'UN QUI NE RISQUE PAS L'ARRESTATION

- **Si tu prévois de risquer l'arrestation** : éteins ton téléphone et confie-le à ta personne de soutien désignée avant le déploiement.
- **Si tu as besoin d'un téléphone pendant l'action** : les personnes qui ont un rôle de soutien (tactique, street medic, désescalade, etc.) peuvent avoir besoin d'un téléphone pendant l'action. Selon l'organisation de l'action et l'imprévisibilité des flics, ces personnes pourront ou non partir quand le risque d'arrestation augmente.
  - Si l'organisation de ton action le permet et que tu as besoin de ton téléphone jusqu'à la dernière minute, confie-le à quelqu'un à ce moment-là.
  - Si tu as besoin de ton téléphone et que tu ne peux pas le confier à quelqu'un, assure-toi de l'éteindre complètement avant une arrestation.

Après l'action

Après l'action, supprime les docs de préparation et les groupes Signal

Les vieilles discussions et les vieux docs peuvent encore être lus si un téléphone est saisi ou si un compte fait l'objet d'une réquisition plus tard.

Une fois l'action terminée, tu n'as plus besoin des documents et des discussions que vous avez créés. Plus ils traînent, plus ils risquent de finir entre les mains des flics, via un téléphone saisi, un subpoena ou un·e indic dans le groupe.

Avant l'action, fixe un plan de nettoyage avec ton groupe. Mets en place un système de responsabilité partagée pour que tout le monde aille jusqu'au bout.

> **Si quelqu'un a été arrêté·e ou inculpé·e, vérifie avec ton équipe de soutien juridique ou un·e avocat·e avant de supprimer quoi que ce soit.** Supprimer des données après avoir appris l'existence d'une enquête, d'un subpoena ou d'inculpations peut être considéré comme une destruction de preuves, ce qui est un délit à part entière. C'est une raison de plus pour activer les messages éphémères avec un délai court avant l'action : comme ça, la plupart des messages auront déjà disparu.

COMMENT FAIRE LE MÉNAGE APRÈS UNE ACTION

1. **Supprime les documents.** Ça inclut les docs de préparation, les docs Proton/CryptPad, les tableurs, les formulaires de soutien aux personnes arrêtées et toutes les notes écrites. Ensuite, vide la corbeille.
2. **Ferme les groupes Signal** : les groupes Signal peuvent être utiles pour continuer à s'organiser, mais la liste des membres représente aussi un risque pour tout le monde si le téléphone de quelqu'un est saisi un jour. Pour continuer à s'organiser, pense plutôt à faire passer tout le monde dans un groupe plus large réservé aux annonces, au lieu de garder ce petit groupe actif.
   - Poste un message pour prévenir tout le monde que le groupe va être fermé, et demande à chacun·e de supprimer la discussion de son téléphone. Retire toi-même chaque membre pour être sûr·e que ce soit fait.
   - Supprime la discussion de ton propre téléphone : Signal → Écran principal → Balayer la discussion vers la gauche → **Supprimer**. (Ça ne supprimera pas le groupe des téléphones des autres, seulement du tien. Par contre, les messages éphémères s'effaceront automatiquement des téléphones de tout le monde.)
3. **Si tu n'es pas admin,** quitte ET supprime le groupe et encourage tout le monde à faire pareil.
4. **Passe à la déchiqueteuse toutes les notes papier**, cartes ou listes.

En savoir plus

- CLDC - Expect the Unexpected: Secure Your Phone Against Confiscation or Loss — protéger ton téléphone contre la confiscation ou la perte[24] (2021)
- Freedom of the Press Foundation - What to do if your phone is seized by the police — que faire si les flics saisissent ton téléphone[25] (2016)

Continue d'apprendre avec ces guides

Checklist de sécurité pour les organisateur·ices d'actions

Sécurité physique, numérique et juridique pour l'organisation d'actions de désobéissance civile où les gens risquent l'arrestation.

Organiser une soirée sécurité

Un modèle d'ordre du jour pour faire les checklists ensemble avec ton groupe.

Se préparer pour une manif

Pour toutes les personnes qui vont en manif.

Liens

1. activistchecklist.org/fr/contribute/
2. activistchecklist.org/fr/action-safety/
3. activistchecklist.org/fr/protest/
4. activistchecklist.org/fr/secondary/
5. activistchecklist.org/fr/party/
6. unwall.app/www.wired.com/story/ice-is-running-one-of-the-largest-anti-left-surveillance-operations-in-us-history/
7. signal.org
8. signal.org/download/
9. activistchecklist.org/fr/signal/
10. support.signal.org/hc/en-us/articles/360007320771-Set-and-manage-disappearing-messages
11. proton.me/drive/docs
12. activistchecklist.org/fr/proton/
13. proton.me
14. drive.proton.me
15. cryptpad.fr
16. jotform.com
17. activistchecklist.org/fr/ice/
18. eff.org/deeplinks/2026/04/google-broke-its-promise-me-now-ice-has-my-data
19. nlg.org/chapters-2/
20. activistchecklist.org/fr/updates/
21. support.microsoft.com/en-us/windows/turn-on-automatic-app-updates-70634d32-4657-dc76-632b-66048978e51b
22. strongphrase.net/passcode
23. ssd.eff.org/module/attending-protest
24. cldc.org/expect-the-unexpected-secure-your-phone-against-confiscation-or-loss/
25. freedom.press/training/mobile-security-for-activists-and-journalists/