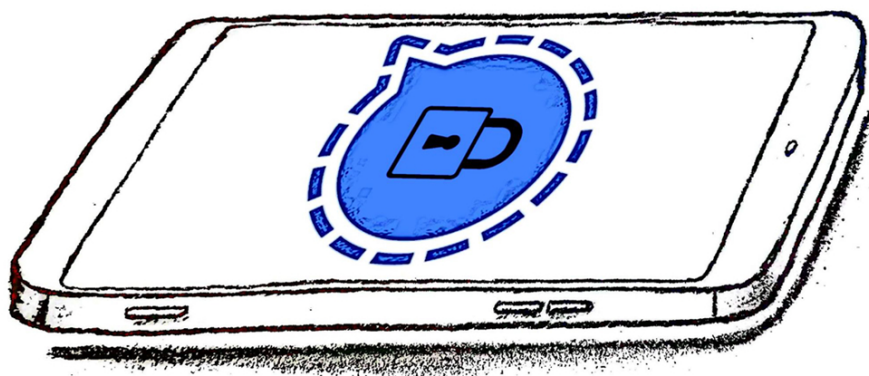


Sécuriser Signal : un guide à destination des militant-es



7 niveaux de protection adaptés
à ton modèle de menace

Mars 2026

Introduction

Salut ! Voilà un petit zine pour t'apprendre à utiliser Signal de manière aussi sécurisée que possible !

Ici, on est vraiment dans une approche de **réduction des risques** : aucune solution n'est parfaite ou suffisante à elle seule, c'est la **combinaison** de ces différentes approches qui permet de se protéger au mieux.

On a découpé ce guide en **niveaux** : les **premiers niveaux** sont vraiment **très abordables**, et on t'invite vraiment à les lire même si tu te sens complètement à la ramasse vis-à-vis de tout ce qui touche à internet, à l'électronique, au numérique... On pense que c'est vraiment une **bonne porte d'entrée dans les idées et les pratiques de sécurité numérique**, et tu peux commencer par les premiers niveaux et revenir plus tard voir les suivants quand tu le sens ! Tout est une question d'**habitude** à prendre. Ces niveaux sont aussi adaptés à différents **modèles de menace** (*threat model*) : les niveaux les plus hauts correspondent à des trucs à mettre en place si tu penses être particulièrement menacé-e ou surveillé-e¹.

Cependant, n'oublie pas que **la sécurité ne concerne jamais qu'une seule personne : tu échanges avec des gens et tu impactes donc leur niveau de sécurité**. Pour cette raison, il est **toujours important de se protéger même si on pense ne pas être spécialement menacé-e** : ça permet de **participer à l'anonymat de nos camarades** et à **les protéger**.

Plus encore, il ne faut pas que ces conseils te fassent te sentir surpuissant-e : **chaque outil est faillible** et le sentiment de confiance déraisonné pousse souvent à faire ou dire des bêtises. Il faut donc **utiliser Signal** comme chaque autre application de messagerie : **avec prudence**.

Aussi, avant d'entrer dans le vif du sujet, **on voudrait t'inviter à t'organiser autant que possible en dehors des technologies**. On fait ce zine pour t'aider à réduire les risques liés à la communication en ligne, mais on pense qu'il faut réussir à s'organiser autant que possible sans ces supports informatiques, surtout quand il s'agit de discuter de sujets sensibles t'exposant à un gros risque de répression. Un support informatique pourra toujours être compromis, et tu pourras toujours faire une erreur en le maniant, alors qu'il est **beaucoup plus difficile d'aller espionner une conversation privée dans un bois**² par exemple.

Pour info, on a choisi de ne pas insérer de captures d'écran dans le zine pour ne pas l'allonger inutilement. On pense avoir assez bien décrit les étapes à suivre pour que tu n'en aies pas besoin, mais si jamais les explications n'étaient pas claires on t'invite à jeter un œil à <https://ssd.eff.org/fr/module/guide-pratique-utiliser-signal>, qui explique très bien comment configurer Signal et l'illustre avec de jolies **captures d'écran**. On espère que ça t'aidera !

1 A propos des modèles de menace, voir : <https://www.privacyguides.org/fr/basics/threat-modeling/#essayez-vous-meme-protéger-vos-biens> ; et <https://www.notrace.how/resources/fr/#threat-modeling-fundamentals>

2 Voir aussi les réflexions de [notrace.how/resources/download/signal-fails/signal-fails-fr.pdf](https://www.notrace.how/resources/download/signal-fails/signal-fails-fr.pdf)

Sécuriser Signal : le guide en 7 niveaux

Niveau 1 : Starter pack

Les **règles de base, impossible de survivre sans**. Un peu de réduction des risques avec un minimum d'efforts : 3 minutes max pour réaliser tout ça et aucune contrainte dans l'utilisation quotidienne de l'application.

- Garde l'application **à jour**, ça t'évitera des failles de sécurité.
- **Pas de photo de profil** qui te représente toi, tes ami-es ou tes proches. Encore mieux : pas de photo de profil du tout.
- **Pas de nom Signal qui soit ton vrai nom ou prénom** ! Le but c'est l'anonymat.
- **Pas de possibilité de te trouver sur Signal à partir de ton numéro de téléphone**. Pour configurer ça, tu ouvres Signal, tu cliques sur l'icône de ton profil en haut à gauche, puis tu vas dans les "Paramètres". Dans la rubrique "Confidentialité" de ces paramètres, tu cliques sur "Numéro de téléphone" et tu sélectionnes "Personne" pour "Qui peut voir mon numéro" ET pour "Qui peut me trouver grâce à mon numéro".
- **N'autorise pas à Signal l'accès à tes contacts et photos de contacts**. Sur iPhone, va dans les paramètres de Signal, puis "Conversations", et désactive le partage des contacts et des photos du carnet d'adresse. Sur Android, les photos du carnets d'adresse se gèrent au même endroit, mais pas les contacts, qui se gèrent dans les paramètres du smartphone, pas de Signal : "Paramètres", puis "Applications", puis "Informations sur l'application Signal", et enfin "Autorisations".

Là tu dois te dire "Euh d'accord mais comment les gens vont faire pour m'ajouter sur Signal maintenant s'ils ne peuvent pas me trouver avec mon numéro ?". Et c'est génial car c'est exactement ce dont parle la prochaine section !

Niveau 2 : On s'échauffe

- Vu que désormais on ne peut pas te trouver sur Signal avec ton numéro de téléphone, tu dois **créer un nom d'utilisateur-ice**. On ne parle pas de ton pseudo Signal que les gens voient quand iels ont une conversation avec toi. Le nom d'utilisateur-ice, lui, n'est pas configuré par défaut et n'est pas visible pour les autres. Pour le configurer, ouvre Signal, clique sur l'icône de ton profil en haut à gauche, vas dans "Paramètres" et clique sur la rubrique tout en haut, où il y a l'icône de ton profil, ton nom signal et ton numéro de téléphone³. Dans cette section "Profil", cherche la troisième rubrique,

3 Même si tu as bien sélectionné "Personne" pour "Qui peut voir/me trouver grâce à mon numéro" avant, c'est normal que toi tu puisses toujours voir ton numéro de téléphone ici.

représentée par un @. À cet endroit, tu peux configurer (ou modifier) un nom d'utilisateur-ice, qui a la structure **@mot.chiffre** (exemple : @acab.1312). C'est un truc vraiment important : une fois ce nom d'utilisateur-ice configuré, tu pourras le donner aux gens qui voudraient t'ajouter sur Signal au lieu de leur donner ton numéro de téléphone ! C'est **hyper important de ne pas donner son numéro à n'importe qui car il est super facile de connaître ta vraie identité une fois qu'on a ton num'**. Si la personne galère à t'ajouter avec ton @, il faut qu'elle clique sur l'icône "Écrire un nouveau message"⁴ et qu'elle rentre ton @ dans la section "Recherche par nom d'utilisateur".

- Utilise ce @ comme un nom **éphémère** et **change le régulièrement**, au moins dès que tu l'as donné à quelqu'un-e et que la personne t'a écrit. Avoir un @ que tu changes souvent permet de diminuer le risque que les keufs relient ce @ à ton numéro de téléphone, et donc à ta vraie identité⁵. Surtout, **ne rends pas ce nom d'utilisateur-ice public**.
- Dans les paramètres, rubrique "Compte", **définis un PIN** et active les **rappels** de code PIN pour le mobiliser régulièrement et ne pas l'oublier : sans le code PIN, aucun moyen de **restaurer ton compte**. Ainsi, si tu supprimes l'application et que tu la réinstalles, Signal te demandera le PIN associé à ton compte pour te reconnecter.
- Active aussi le **blocage d'inscription** pour que **personne ne puisse réenregistrer ton numéro de téléphone sur Signal sans ce code PIN**. Si tu te retrouves en garde à vue avec ton téléphone et que tu avais désinstallé Signal en sortant de chez toi, avoir un PIN empêchera que les keufs réinstallent Signal sur ton téléphone et récupèrent la liste de tes boucles de discussions et de tes contacts⁶. Ça limite aussi les chances que tu te fasses hacker ton compte.
- Toujours dans la rubrique "Confidentialité" des paramètres, tu peux **activer le "Verrouillage de l'écran"** et configurer un délai avant verrouillage de l'écran. De cette manière, si tu n'as pas utilisé Signal pendant x minutes/heures (selon le délai défini) et que tu veux ouvrir l'application, Signal te demandera ton **code de téléphone**⁷. Adapte ce délai à ton modèle de menace : plus tu penses être menacé-e, plus ce délai doit être court. Ça peut être pénible au quotidien mais ça évite que quelqu'un-e puisse accéder à toutes tes conversations si tu laisses ton téléphone déverrouillé sans surveillance (ce qui, soit dit en passant, est une très mauvaise idée) ou que tu le prêtais. C'est aussi une bonne pratique d'avoir un **téléphone qui se verrouille rapidement** de manière générale.

Niveau 3 : Road to l'anonymat

4 Sur Android c'est une icône en forme de stylo en bas à droite de la page principale d'affichage des conversations, sur iPhone c'est une icône en forme de stylo en haut à droite sur la même page.

5 Voir : <https://znetwork.org/znetarticle/signals-new-usernames-help-keep-the-cops-out-of-your-messages/>

6 Encore mieux : **n'emmène pas ton téléphone en manif**, ça t'évitera des problèmes.

7 Plutôt qu'un code à 4 chiffres (souvent proposé par défaut), utilise un code à 10-12 chiffres, voire un code alphanumérique. Plus un mot de passe est long et aléatoire, plus il est robuste. Surtout n'utilise pas la biométrie.

- Sélectionne un **délai de messages éphémères** (Paramètres, rubrique "Confidentialité"). En faisant ça, toute nouvelle conversation que tu initieras sera par défaut effacée au bout du délai que tu auras configuré. Avec Signal, il ne faut pas s'attacher ! **La sécurité avant tout : c'est une très bonne chose que les messages disparaissent rapidement.** Pour info, cette fonctionnalité supprime les messages échangés mais Signal garde en mémoire que tu as déjà échangé avec la personne dont les échanges ont été effacés : tu n'as donc pas perdu son contact, la discussion a juste été déplacée tout en bas de la liste de tes conversations.
- **Restreins le contenu des notifications.** Pour ça, va dans la rubrique "Notifications" des paramètres, et regarde la section "Contenu des notifications". Sélectionne "Ni nom, ni contenu", pour que les messages Signal que tu reçois ne puissent pas s'afficher sur l'écran de verrouillage de ton téléphone.
- **Désactive aussi les aperçus de liens** (dans les paramètres, rubrique "Conversations"), car pour générer cet aperçu, Signal communique avec le site d'où vient le lien, et cela pourrait constituer une faille de sécurité⁸.
- **Si une personne présente sur un groupe Signal se retrouve en GAV, retire-la du groupe.** Par anticipation, **accordez toujours les droits d'administrateur à toutes les membres** d'un groupe pour que tout le monde ait la possibilité de retirer la personne qui est en GAV.

Niveau 4 : Petit-e toto deviendra grand-e

- Plus haut, on parlait du fait de configurer un nom d'utilisateur-ice (qu'on appelle aussi @) pour ne pas donner son numéro de téléphone. C'est effectivement très important, mais **l'usage le plus sécurisé de Signal consiste à :**
 - **ne pas avoir de numéro téléphone visible**
 - **ET ne pas avoir de @ configuré.**

Et là tu te dis : "Mais c'est impossible, je ne vais pouvoir communiquer avec personne si je fais ça !"

Et on t'explique : plus haut, on te disait qu'il faut régulièrement changer ce @ pour éviter que les keufs arrivent à relier ton compte Signal à ta vraie identité. On va imaginer une petite histoire pour illustrer et mieux comprendre ça : après une AG intense en propositions démocratiques, tu brûles d'envie de t'organiser avec les individu-es les plus chaud-es de ta région. Tu n'es pas assez inconscient-e pour donner ton num au premier venu, alors tu donnes à Toto1312 ton @ pour qu'il t'ajoute sur Signal. Les semaines passent, tu oublies de changer ton @ et il s'avère que Toto1312 était en fait... un keuf infiltré ! Il a donc eu plusieurs semaines pour demander à Signal à quel numéro appartenait le compte relié au @ que tu lui avais donné. Signal a bien essayé de faire traîner la requête

8 Pour être exact-es, la communication avec le site en question se fait via un serveur proxy, ce qui ajoute une sécurité importante (<https://signal.org:8443/blog/i-link-therefore-i-am/>). En 2023, la rumeur d'une vulnérabilité critique vis-à-vis de cette fonctionnalité s'est toutefois répandue mais a été démentie par Signal après analyse (<https://thehackernews.com/2023/10/signal-debunks-zero-day-vulnerability.html>). Cependant, toute fonction ajoute de la surface d'attaque, c'est-à-dire de nouveaux moyens de compromettre un système informatique. Cette fonctionnalité étant anecdotique, on te conseille donc de la désactiver.

pour tenter de te sauver les fesses, mais iels ont dû lâcher le morceau : les keufs ont donc ton numéro, grâce auquel ils obtiendront ton identité civile en moins de deux, et patatras, on t'attrape pour une erreur aussi bête que ça.

Du coup, **la pratique la plus sécurisée consiste à ne jamais avoir de @ configuré**. Pour que des gens puissent quand même t'ajouter sur Signal, configure un @ (ultra éphémère du coup), donne-le, demande à la personne de t'écrire immédiatement, et **supprime-le** une fois que c'est fait. **Ça évite que tu oublies de changer ce @** et que tu te retrouves dans la situation imaginée précédemment ! En effet, ici même si la personne à qui tu viens de donner ton @ est en réalité un-e keuf infiltré-e, le temps qu'elle fasse la demande auprès de Signal pour savoir à quel numéro appartient ce @, tu l'auras déjà supprimé. Aussi, il n'apparaîtra donc plus dans la base de données de Signal, qui ne pourra répondre à la requête des keufs que par un "désolé-es, le @ que vous demandez n'est pas attribué". Cela participe à protéger solidement ton anonymat.

- Active l'option "**Toujours relayer les appels**" dans la rubrique "Confidentialité", puis "Paramètres avancés". Cela permet que les appels que tu reçois soient relayés par un serveur Signal afin de **ne pas révéler ton adresse IP à la personne qui t'appelle**.
- Vérifie le **numéro de sécurité** de tes contacts. C'est la meilleure **protection contre une interception des messages**. C'est assez simple à faire et plus facile en face-à-face. Ouvre ta conversation avec la personne que tu veux vérifier et va dans les Paramètres de la conversation, puis dans Afficher le numéro de sécurité. Il faut que ton contact fasse pareil. Là, tu peux soit scanner le QR code, soit comparer les numéros qui s'affichent sur vos deux écrans. Si ça colle, c'est vérifié !

Toujours dans la rubrique "Confidentialité" des paramètres :

- **Désactive les indicateurs de saisie** (=les 3 points qui montrent que tu es en train d'écrire) **et les confirmations de lecture**. Ça permet de **diminuer les éléments de ton trafic Signal que les keufs pourraient espionner et analyser pour essayer de les relier à ta vraie identité**. En gros, imaginons qu'un keuf te soupçonne d'être derrière un certain compte Signal. Pour vérifier ça, il surveille le trafic de ta connexion internet et t'envoie des messages Signal. Il va alors regarder si les accusés de lecture ou les indicateurs de saisie correspondent aux échanges de ton point d'accès internet avec les serveurs de Signal⁹, et si c'est le cas il confirme alors les soupçons qu'il avait sur toi. Ça correspond donc à un certain type de menace, mais c'est important à prendre en compte.
- **Active le mode "Clavier incognito"**, pour désactiver l'apprentissage personnalisé du clavier¹⁰.
- **Active la sécurité de l'écran pour empêcher les captures d'écran dans Signal**. Comme ça, si jamais ton téléphone était infecté par un logiciel

9 Au moment où on écrit ce zine, impossible de remettre la main sur les sources qu'on avait à ce sujet. Si vous en avez, n'hésitez pas à nous les envoyer à zinesignal@systemli.org !

10 N'est malheureusement pas toujours disponible sur les iPhone

espion (*spyware*), ce dernier ne pourrait pas faire de capture d'écran de tes conversations Signal.

- **Quand tu crées un nouveau groupe Signal, donne-lui un but précis. Quand celui-ci est atteint, il vaut mieux que tout le monde le quitte et supprime la conversation correspondante.** Pour quitter le groupe : quand tu es dans la discussion, tu cliques sur les 3 petits points en haut à droite, puis "Paramètres du groupe". Ensuite, descends tout en bas et clique sur "Quitter le groupe". Pour supprimer la conversation associée : dans la liste de tes conversations, tu restes appuyé-e sur celle que tu veux supprimer (Android) ou tu glisses la conversation vers la gauche (iOS) jusqu'à faire apparaître un petit menu. Dans celui-ci, clique sur "Supprimer". Si tu ne fais pas ça, elle continuera d'apparaître dans ton historique de conversations même après avoir quitté le groupe.
- Dans la même optique, **supprime de tes contacts les gens avec qui tu ne parles pas ou plus.** Pour cela, clique sur l'icône pour écrire un nouveau message. Ça t'amène à la liste des personnes à qui tu peux écrire. À cet endroit, reste appuyé-e sur le contact que tu veux supprimer jusqu'à l'apparition d'un menu. Dans ce menu, clique sur "Supprimer". Comme ça, si les keufs arrivent à avoir accès à ton Signal, ils n'auront pas l'intégralité des gens avec qui tu as été en contact.

Niveau 5 : Molly

Si ton téléphone est sous **Android**, tu peux utiliser **Molly**¹¹ à la place de Signal. Molly est une variante¹² de Signal qui a plusieurs **avantages de sécurité**. Il y a un faisceau d'indices nous poussant à avoir confiance en Molly, mais l'application n'a **pas été auditée**¹³ à ce jour. **En termes d'utilisation, ça ne change rien du tout, promis** : tu peux utiliser Molly sans changer de compte Signal, tu peux synchroniser Molly avec Signal sur ton ordinateur¹⁴, et communiquer avec les gens qui utilisent Signal ou Molly sans souci. Il y a plusieurs manières de l'installer, et on te recommande de le faire via la plateforme Accrescent¹⁵, sorte de mini-playstore du libre.

Avec Molly, on te conseille plusieurs trucs :

- **Chiffre la base de données de messages au repos** (Paramètres, section "Confidentialité", "Chiffrement de la base de données"). Ainsi, quand l'appli est verrouillée, il est impossible d'avoir accès aux messages. Comme ça, même si des keufs craquent le mot de passe de ton téléphone, ils ne pourront pas lire le contenu de tes discussions Molly.
- Pour chiffrer la base de données des messages, utilise une **phrase de passe complexe et aléatoire** (que tu peux générer avec KeePassXC ou

11 <https://molly.im/>

12 Pour les nerds qui lisent ça, oui on sait que le bon terme c'est *fork*, mais on fait de la vulgarisation là

13 Ça signifie qu'il n'y a pas d'entité extérieure qui a formellement inspecté le code et fait des retours à Molly sur d'éventuelles failles. L'application est toutefois open source et a été inspectée par des milliers de gens.

14 Si ton ordinateur n'est pas chiffré, il est plus facile d'avoir accès à tes conversations Signal avec la version ordinateur que smartphone, par exemple en cas de perquisition.

15 <https://accrescent.app/>

bien <https://diceware.fr> par exemple) que tu ne retiendras que dans ta tête ou dans un gestionnaire de mots de passe comme KeePassXC¹⁶. Tu peux à tout moment **changer** ton mot de passe de déverrouillage dans les paramètres (section "Confidentialité", "Modifier la phrase secrète"). Fais-le dès maintenant si tu avais configuré un mot de passe de déverrouillage trop simple !

- **Active le verrouillage automatique des messages en cas d'inactivité** (Paramètres, section "Confidentialité", "Verrouillage automatique"). Grâce à ça, si tu ne déverrouilles pas ton téléphone pendant un certain temps (personnalisable dans les paramètres, section "Confidentialité", "Durée de verrouillage de l'appareil"), Molly se re-verrouille (le même système est dispo sur Signal aussi mais uniquement avec le code de ton téléphone). Si tu n'actives pas cela, le chiffrement que tu as configuré juste avant ne sera activé que quand tu **éteindras** ton téléphone. L'avantage de ce verrouillage en cas d'inactivité est que si quelqu'un te vole ton téléphone ou que tu te retrouves en GAV avec ton téléphone¹⁷, les messages seront à nouveau chiffrés. On te conseille de **régler la durée de verrouillage automatique sur une durée assez courte** (entre 2 et 4 heures par exemple) pour que le **verrouillage** se fasse assez **rapidement** en cas de besoin. Cette durée est aussi à adapter en fonction de ton modèle de menace.

Niveau 5 + : Molly max

- **Installe Orbot** (disponible sur le Play Store) **et force Molly à utiliser Orbot** (Paramètres, section "Réseau", "Utiliser un proxy", "Tor via Orbot"). Cela permet d'**acheminer tout le trafic de Molly via le réseau Tor**, réseau d'**anonymisation** maintenu par des milliers de personnes dans le monde. Cela rend beauuuucoup plus difficile l'analyse de ton activité et la **cartographie des réseaux militants** dont tu fais partie, qui reste relativement accessible pour l'État si on ne met pas cela en place (et qui est très facile si on utilise Signal et non Molly). La cartographie d'un réseau militant signifie savoir qui parle avec qui, quelles sont les personnes centrales ou les lieux d'organisation dans un réseau donné, etc.¹⁸
- Tu peux **configurer Molly pour utiliser UnifiedPush et avoir la main sur le système de notifications**. Si tu fais ça, il vaut mieux que ce soit avec un **serveur que tu administres toi-même**, et non une instance publique de UnifiedPush¹⁹.
- Tu peux aussi **utiliser Orbot directement avec Signal** et forcer l'application à acheminer son trafic par le réseau Tor. Dans ce cas, ça se configure directement dans les paramètres d'Orbot, où il faut cocher "Signal" dans la liste des applications qu'Orbot prend en compte²⁰.

16 <https://keepassxc.org/>

17 On l'a déjà dit mais on le répète : emmène pas ton téléphone en manif, ça t'évitera des problèmes

18 <https://www.notrace.how/threat-library/fr/techniques/network-mapping.html>

19 <https://github.com/mollyim/mollyim-android?tab=readme-ov-file#unifiedpush>

20 Avec Signal, cette configuration se fait de manière extérieure à l'application et est donc moins fiable : si tu perds la connexion à Orbot, ton trafic ne passe juste plus par Tor. Alors qu'avec Molly, le trafic est carrément bloqué, il n'y a pas de fuites. Pour contourner ce problème avec Signal, il faut forcer l'intégralité du trafic du téléphone à passer par Tor (très peu pratique).

Niveau grave déter (aussi appelé niveau 6) :

- Il est possible de **configurer un compte Signal/Molly²¹ avec un numéro qui n'est pas le tien**, soit en achetant (en cash) une **SIM prépayée**, soit en **utilisant le numéro de quelqu'un-e que tu connais et qui n'utilise pas Signal** (je sais pas, ta grand-mère par exemple ?). Chacune de ces solutions a ses inconvénients :
 - **Utiliser le numéro de quelqu'un-e que tu connais te rend plus facilement traçable**. Tu n'es pas identifié-e personnellement, mais un-e de tes proches l'est. Potentiellement, ça peut lui attirer des emmerdes ou, à terme, permettre aux keufs de t'identifier.
 - Avec une **SIM prépayée achetée en cash que tu n'as jamais mise dans un téléphone relié à ton identité**, il est impossible de relier ton compte Signal à ta vraie identité par ton numéro de téléphone. Cependant, vu que le but est de **ne pas utiliser ce numéro** à part pour la configuration du compte Signal, il **va rapidement être considéré inactif**, et il risque d'être réattribué à une autre SIM²². Il est donc possible que tu te fasses "voler" ton compte Signal si quelqu'un-e achète la SIM à laquelle ce numéro a été réattribué et qu'iel se crée un compte Signal avec. Le code PIN participe à réduire ce risque, mais ce n'est qu'un code à 4 chiffres - donc très peu robuste²³.

Dans tous les cas : ces deux configurations imposent que tu **ne puisses pas avoir sous la main le numéro auquel est relié ton compte Signal**. Cela peut te poser problème puisque Signal envoie généralement des codes de vérification à ce numéro quand tu veux faire certaines opérations (comme restaurer un compte ou te reconnecter).

- Avec une **SIM prépayée**, tu peux aussi vouloir **utiliser Signal uniquement sur Tails²⁴**. Il faudra que tu **installés l'application sur ton stockage**

21 Dans cette section, on écrira "Signal" par facilité mais tout ce qu'on dit est évidemment aussi valable pour Molly.

22 À partir de 90 jours d'inactivité pour une Lyca, extensible à un an sous conditions pour 5€ (voir site) ; 40 jours d'inactivité pour une SYMA.

23 Voir la fin de cette section pour plus de détails sur les recharges de SIM prépayées.

24 Tails étant un système d'exploitation basé sur la préservation de l'anonymat, il est absurde et dangereux de l'utiliser pour faire tourner un compte Signal relié à ta vraie identité. Voir <https://tails.net/index.fr.html>

persistant et que tu le configures pour qu'il **garde en mémoire les paramètres de l'appli**. Cependant, si tu n'utilises pas ton compte Signal sur Tails pendant **1 mois**²⁵, l'appareil sera considéré inactif et la **session sera supprimée**. Il te faudra te reconnecter (et avoir la SIM sous la main pour recevoir le code de vérification), ce qui peut poser problème si tu t'es entre temps débarassé-e de la SIM.

- Si tu utilises aussi **Signal sur ordinateur** et qu'avoir Signal sur Tails le rend trop inaccessible, tu peux aussi **l'installer dans une machine virtuelle Whonix**²⁶. Comme pour Tails, **l'intégralité de ton trafic Signal depuis l'ordinateur sera acheminé à travers Tor**, rendant plus difficile l'analyse de ton activité et la cartographie des réseaux dont tu fais partie. Par rapport à Tails, selon ta situation, cela peut garder Signal davantage **accessible** et facile pour une utilisation régulière. Comme tout le reste, ces choix sont à adapter en fonction de ton modèle de menace.

Petit point sur les SIM prépayées :

Concernant les **SIM prépayées**, on a expliqué plus haut que le **numéro** qui leur était attribué pouvait être considéré **inactif** s'il n'était pas utilisé pendant plusieurs mois et risquait alors d'être **réattribué**. Pour lutter contre ça et être sûr-e de garder ton numéro, il est possible d'**alimenter régulièrement ta SIM prépayée en achetant des recharges en cash** dans un taxiphone ou dans n'importe quel tabac qui propose des recharges de la même marque que ta SIM.

Une fois la recharge achetée, tu dois la charger sur le téléphone (généralement en envoyant le code de ta recharge au numéro dédié que t'aura donné l'opérateur téléphonique à l'achat). Indépendamment de la recharge et pour sécuriser le numéro, il faut que tu t'en **serves** régulièrement (tous les mois par exemple pour une SYMA). Au maximum, essaye de t'en servir **loin de chez toi, pas toujours au même endroit, et en envoyant des messages aléatoires à des numéros aléatoires**.

Surtout, quand tu utilises ta SIM, il faut que tu le fasses uniquement avec **un téléphone dans lequel tu n'as jamais mis de SIM à ton nom !** Sinon le **numéro IMEI**²⁷ de ce téléphone est **relié à cette ancienne SIM** et cela brise l'anonymat que tu essayes de mettre en place. On privilégiera donc un téléphone poubelle, dédié à cet usage uniquement²⁸.

Pour être tout à fait honnête, il est **carrément possible de garder un même numéro pendant des mois sans le recharger ou l'utiliser** : la réattribution du numéro n'est pas automatique après plusieurs semaines/mois d'inactivité. Cependant, ça **peut** arriver et il est donc toujours plus sûr de s'en prémunir.

²⁵ <https://support.signal.org/hc/en-us/articles/360007320551-Linked-Devices>

²⁶ <https://www.whonix.org/>

²⁷ https://fr.wikipedia.org/wiki/International_Mobile_Equipment_Identity

²⁸ Si tu penses utiliser un vieux téléphone à clapet ou à touches pour ce faire, sache que les vieux téléphones construits pour fonctionner en 2G ne seront bientôt plus connectés au réseau téléphonique.

Message de fin

Certaines des pratiques conseillées dans ce zine peuvent te paraître difficiles à mettre en place, ou rendant l'usage de Signal trop pénible. Encore une fois, **tous ces choix sont à accorder à ton modèle de menace**. Mais si le tien est très élevé et que tu rechignes quand même à ajouter des couches de sécurité, demande-toi s'il vaut mieux se faire un peu chier à chaque fois que tu utilises Signal ou bien augmenter ses chances de passer 10 ans en prison (ou même juste 92h dans les sous-sols de la SDAT #pasfun). Et encore une fois, il ne faut pas sous-estimer la rapidité avec laquelle une nouvelle pratique peut devenir une **habitude** à laquelle on ne pense même plus. **Essaie pour voir !**

Il y a aussi sûrement d'autres pratiques importantes à mettre en place, on a essayé de donner une **vue d'ensemble** de ce qui était possible mais on ne prétend pas que cela soit exhaustif. N'hésite donc pas à **fouiller dans les paramètres de Signal** et à **chercher ce qui te semble le plus adapté à ton modèle de menace** notamment.

On veut aussi répéter qu'**il est important de s'organiser autant que possible en dehors des technologies de communication en ligne**, qui sont nettement plus susceptibles de garder des traces exploitables par l'État d'une discussion qu'un face-à-face dans un lieu désert. Plus le risque de répression est grand, plus il est important de s'organiser sans support informatique.

Et surtout, même une fois tous ces conseils mis en place, **il ne faut jamais se croire invincible** : le problème avec un ordinateur se situe très souvent entre la chaise et le clavier (ça veut dire que c'est toi). La partie la plus faillible d'un système information est la composante humaine, et la plupart des gens qui se font coffrer n'ont pas été espionné-es pendant des mois par la NSA : iels ont simplement fait des erreurs d'inattention ou d'excès de confiance. C'est important à garder en tête.

Si des erreurs ou des oublis se sont glissé-es dans le zine, n'hésitez pas à nous le faire savoir à **zinesignal@systemli.org** ! Vos retours sont précieux. Et bien sûr, vos éventuelles questions sont toutes bienvenues !

Sources & ressources

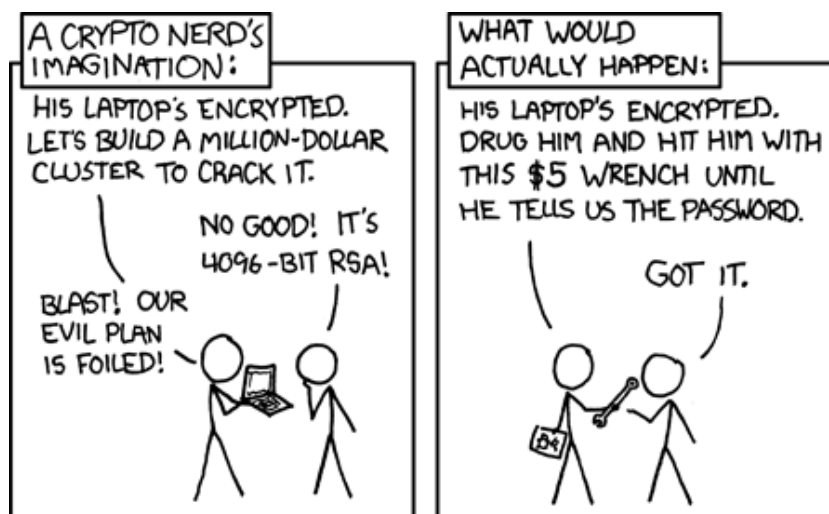
- Le site de Signal sur ce que l'entreprise dit fournir aux institutions judiciaires : signal.org/bigbrother/.
- Cet article qui précise ce que les flics peuvent obtenir à partir d'un @ Signal : znetwork.org/znetarticle/signals-new-username-help-keep-the-cops-out-of-your-messages/
- Ce tutoriel sur la configuration de Signal avec des captures d'écran : ssd.eff.org/fr/module/guide-pratique-utiliser-signal
- Le guide de la téléphonie mobile, avec une section dédiée à Signal : infokiosques.net/spip.php?article1975
- La documentation de Molly : github.com/mollyim/mollyim-android
- Le site de Signal sur la durée pendant laquelle un compte peut rester actif sur un appareil : support.signal.org/hc/en-us/articles/360007320551-Linked-Devices

Applications et outils recommandés :

- Molly (fork/variante de Signal) : molly.im/
- Accrescent (mini Playstore du libre) : accrescent.app/
- KeepassXC (gestionnaire de mots de passe) : keepassxc.org/
- Diceware (générateur de mots de passe) : diceware.fr/
- Whonix (système d'exploitation anonyme qui s'utilise comme une application, et qu'on peut installer sur presque n'importe quel système d'exploitation) : whonix.org/
- Le système d'exploitation Tails : tails.net/index.fr.html
- Tor Browser, Orbot, et toutes les initiatives du Tor Project : www.torproject.org/
- Qubes OS, le système d'exploitation le plus sécurisé à ce jour : qubes-os.org/

Et comme la sécurité numérique c'est super important, quelques autres ressources en vrac sur le sujet :

- Le très massif mais très complet Guide d'Autodéfense Numérique, dont la dernière édition date de 2023 : guide.boum.org/
- Le "Guide de survie en protection numérique à l'usage des militant·es" : infokiosques.net/spip.php?article1849
- Le petit zine "Comment se protéger et protéger nos luttes. Premiers pas dans la mise en place de pratiques de sécurité" : infokiosques.net/spip.php?article2017
- La section "Informatique, défense numérique" d'infokiosques : infokiosques.net/informatique
- Tous les zines du site AnarSec : anarsec.guide/
- Le site de Privacy Guides, qui recommande des outils de protection de la vie privée : privacyguides.org/fr/
- Le guide très approfondi d'AnonymousPlanet : anonymousplanet.org/guide/
- La bibliothèque de menaces du No trace Project : notrace.how/threat-library/fr/
- Le zine *Signal Fails*, un peu daté mais avec des critiques intéressantes de Signal : notrace.how/resources/download/signal-fails/signal-fails-fr.pdf



© xkcd

Questions, suggestions et corrections sont les bienvenues !
Écrivez-nous à zinesignal@systemli.org