Recommandations sur l’utilisation de Signal



Paramétrer son compte Signal

Voici quelques réglages pour protéger son identité et ses échanges sur Signal :

- **Profil :**
  - N'indique pas ton nom/prénom et n'utilise pas une photo de toi sur ton profil
    Explication : ce réglages empêche de t'identifier dans un groupe ou dans les contacts d'une personne
- **Confidentialité :**
  - **Numéro de téléphone :**
    - **Qui peut voir mon numéro :** Personne (sélectionné par défaut)
      Explication : ce réglages empêche de t'identifier dans un groupe par ton numéro de téléphone
    - **Qui peut me trouver grâce à mon numéro :** Personne
      Explication : ce réglage empêche de vérifier ton identité à partir de ton numéro
- **Notifications** :
  - **Désactive les notifications,** ou à minima **"afficher : ni nom, ni message".**
    Explication :iOs enregistre le contenu de toutes les notifications dans un fichier, la police aux USA a déjà pu accéder à tous les messages reçus d'une militante par ce moyen. On ne sait pas si le même système existe sur Android

Rappels avant toute action

1. Eviter au maximum de venir avec son téléphone à une action.

2. Supprimer un maximum de données (signal, mattermost, Email, photos & vidéo, données du presse papier, etc). Sur signal, supprimer les conversations et quitter les groupes non indispensables (actions passées, etc).
3. S’assurer que son téléphone est chiffré.
4. Eteindre son téléphone pour activer le chiffrement. En effet, le premier déverrouillage désactive le chiffrement, il faut donc l'éteindre pour le réactiver.

Pourquoi faut-il supprimer l’application Signal avant une action ou durant l’action avant une possible interpellation ?

Le principal intérêt de Signal est de protéger l'interception à distance des contenus des messages. En utilisant Signal, les messages sont chiffrés de bout en bout, c'est-à-dire que même si une personne 'voit' le message, elle ne pourra pas le lire. Cependant, la protection n'est pas garantie si l'attaquant à un accès physique à un téléphone dans un état non chiffré, soit car le chiffrement a été désactivé avec le premier déverrouillage, soit car le téléphone n'est de base pas chiffré.

Supprimer l’application Signal supprime toutes les données de l’application. Ainsi si les forces de l'ordre ont accès au téléphone dans un état non chiffré elles ne pourront pas obtenir les données.

En cas de suppression de l'application, je veux retrouver les données une fois le risque passé, que puis-je faire ?

Il est possible de créer une sauvegarde chiffrée des données sur le téléphone ou en dehors. Pour cela aller dans: (en passant par Settings > Chats > Chat backups > Turn on). Il faut bien noter dans un endroit sécurisé la passphrase (non accessible par les Forces de l’Ordre). Ainsi si l’application ou le compte signal a été supprimé, lors de la réinstallation on peut utiliser cette sauvegarde en la décryptant via la passphrase et ainsi retrouver ses données.

Les forces de l’ordre ne peuvent-elles pas me demander cette passphrase ?

Si elles le peuvent mais encore faudrait-il qu’elles identifient cette sauvegarde. Même si elle est stockée sur le téléphone, ce n’est pas si simple et on peut donc espérer qu’elles ne l’identifient pas. Il est aussi possible de stocker la sauvegarde en dehors du téléphone. De plus, si vous dites (devant un tribunal, en GAV on ne dit rien) ne plus avoir cette passphrase car vous ne l’aviez pas notée ou que vous l’avez perdu, ce sera une position plus crédible juridiquement car c'est plausible.

Faut-il mieux supprimer l’application ou supprimer son compte signal ?

Signal donne la possibilité de supprimer son compte: Settings > Accounts > Delete account. La différence par rapport à supprimer l’application est qu’en cas de suppression du compte le numéro

de mobile n'est plus répertorié sur les serveurs de Signal. Ainsi, une personne extérieure ne peut pas soupçonner que tu utilises Signal habituellement (en entrant ton numéro dans Signal un.e utilisateur.rice le verra comme non sécurisé). De plus, supprimer son compte quitte automatiquement tous les groupes.

Les failles dans l'outil Cellebrite, outil utilisé par les FDO pour analyser les téléphones remettent-elles en question ces recommandations ?

Non.

Context sur Cellebrite

Cellebrite est un outil utilisé par les forces de l'ordre pour extraire et analyser automatiquement les données d'un téléphone. Pour ce faire, il faut avoir brancher physiquement à l'outil le téléphone allumé et dévérouillé. L'utilisation de Cellebrite est donc par exemple possible dans un cas où un.e militant.e serait amené.e en garde à vue et n'aurait pas son téléphone chiffré.

Notez que sur les versions récente d'Android, le téléphone est chiffré par défaut, jusqu'à ce que vous l'ayez déverouillé une première fois depuis son démarage, même si vous l'avez revérouillé ensuite, il est donc fortement conseillé de l'avoir éteint ou rédémarré avant que les FDOs le récupère, pour qu'il soit chiffré à ce moment là.

Lien avec Signal

Signal a publié cet article disant qu'iels avaient exploité.e.s des failles dans Cellebrite afin de corrompre la donnée collectée. Cette exploitation peut permettre de rendre la donnée collectée lors une analyse automatique du téléphone moins fiable et donc contestable devant un tribunal. Cependant, selon Signal, cette corruption est très loin d'être systématique et il est possible que Cellebrite a pu réparer la faille ou qu'un autre outil d'analyse soit utilisé par les Forces de l'Ordre. De plus, une analyse humaine (en lisant simplement les messages) peut-toujours être réalisée. Ainsi ces failles ne remettent pas en cause le besoin de supprimer Signal et d'avoir le moins de données possibles sur son téléphone.

Autres ressources

Tuto très détaillé sur les bonnes pratiques sur Signal: https://paris-luttes.info/IMG/pdf/zine_signal_ppp.pdf

---

Créé 2023-09-08 20:16:26 CEST par mollusque
Mis à jour 2026-11-23 00:14:24 CET par osmi