

Outil - Communiquer avec Signal

TOUTES LES FICHES

par Nothing 2hide



PUBLIC



PARTICIPANTS



ANIMATEURS



NIVEAU



PRÉPARATION



ACTIVITÉ

Description

Cette fiche permet à l'animateur.rice de se familiariser avec l'application signal.

Objectifs

NA

Matériel

NA

Contenus utilisés

NA

Pré-requis

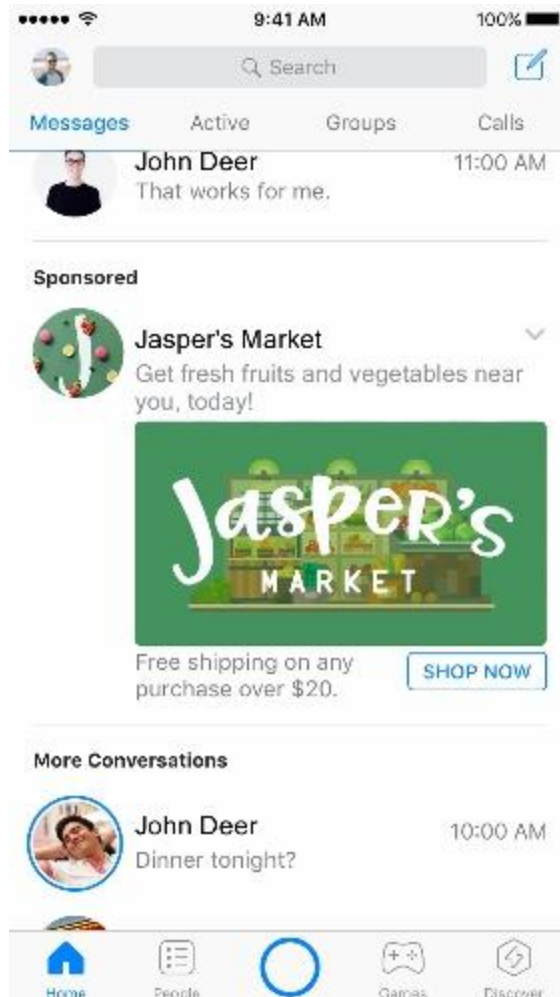
NA

WORKFLOW

1

Introduction au chiffrement des communications

Sachez que vos communications sont une mine d'informations. Vous pouvez être surveillé pour des raisons précises, dans le cadre d'une enquête judiciaire par exemple. Mais, et c'est plus souvent le cas (heureusement), les applications que vous utilisez pour communiquer peuvent récupérer des éléments sur vous et les utiliser pour de la publicité ciblée. C'est le cas de Google / Alphabet avec son service Gmail par exemple qui a utilisé pendant des années des robots pour scanner le contenu des emails de ses utilisateurs et leur servir de la publicité ciblée e fonction des mots clés utilisés dans les mails. [Facebook Messenger "offre" également la possibilité d'afficher des publicités ciblées](#) en fonction du contenu de votre conversation.



Deux personnes discutent de ce qu'elles pourraient manger pour le dîner. Comme par magie, une publicité sur un produit alimentaire apparaît dans la conversation.

Pour vos communications, il y a deux choses à différencier : les communications qui passent par le réseau GSM classique (appel téléphoniques, SMS et MMS), et tout ce qui passe par le réseau Internet, 3G, 4G.

Les appels téléphoniques et les sms sont très faciles à intercepter et surtout à déchiffrer. Quelqu'un de mal intentionné et correctement équipé peut écouter et lire vos échanges, voix ou texte, en temps réel.

Pour les communications utilisant le réseau Internet, là c'est un peu plus compliqué, cela dépend essentiellement de l'application que vous allez utiliser.

Des applications de communications sur smartphone:

- Messenger : n'est pas sécurisé par défaut. Il faut désormais utiliser l'option "[conversation secrète](#)" qui enclenche le chiffrement de bout en bout. Une conversation chiffrée de bout en bout signifie que seul vous et votre interlocuteur disposez des clés de déchiffrement des messages audio ou texte que vous échangez. Ceux-ci sont chiffrés sur votre smartphone puis déchiffrés sur le smartphone de la personne avec qui vous communiquez.
- WhatsApp : permet d'avoir des conversations chiffrées de bout en bout par défaut. Attention cependant : toutefois, les métadonnées – à savoir tel numero Whatsapp a appelé tel autre numéro Whatsapp pendant x temps – sont conservées.
- Skype : permet d'avoir une conversation chiffrée avec son ou ses interlocuteurs cependant celle-ci n'est pas chiffrée de bout en bout par défaut : Microsoft dispose des clés de chiffrement et déchiffrement et peut techniquement avoir accès au contenu de votre conversation. Pour avoir une conversation vraiment confidentielle sur Skype il faut utiliser l'option "démarrer une conversation privée"
- Snapchat : n'offre aucun moyen de chiffrer ses messages. Pire, les messages éphémères de Snapchat peuvent être [techniquement récupérés](#) par la firme
- Telegram : les messages de cette application ne sont pas chiffrés par défaut. Il faut activer l'option "New secret chat" pour chiffrer les messages. Par ailleurs, contrairement à Skype, Messenger et Telegram qui utilisent des méthodes de chiffrement connues donc auditable, Telegram utilise [son propre système de chiffrement](#) que seule la firme connaît.
- ...

Pour préserver sa vie privée, l'une des meilleures applications disponibles à ce jour – et gratuitement qui plus est – c'est [Signal](#).

2

Utilisation de l'application Signal

[Dans une interview donnée au journal Le Monde](#), les créateurs de cette application expliquent s'être fixés comme objectif :

que chaque personne concernée par le respect de la vie privée dans son quotidien ait accès à un service gratuit. On croit que tout le monde a le droit de communiquer librement et en sécurité.

Pas de panique, il n'est pas nécessaire d'avoir bac +8 en espionnage. Les applications chiffrées sont accessibles à tous. L'équipe de Signal assure d'ailleurs vouloir :

que tout le monde ait accès à des communications d'une sécurité avancée, qui soient aussi faciles et accessibles qu'un banal appel téléphonique.

Signal chiffre la voix et les messages textes. Vous pouvez appeler, envoyer des messages vocaux ou texte. Vous pouvez également envoyer des pièces jointes (photo, PDF, etc).

Maintenant, place à la prise en mains. Il s'agit d'installer l'application :

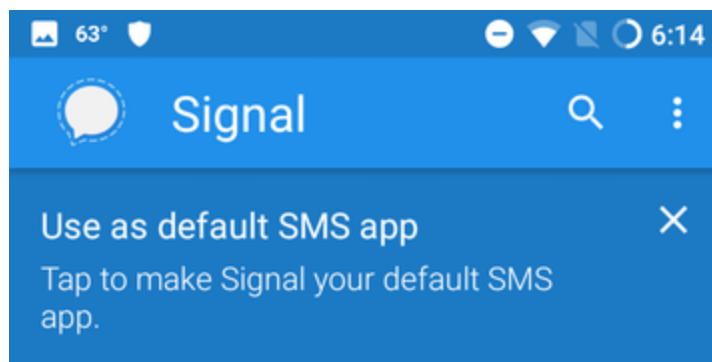
- pour les possesseurs d'un android, direction [Google play](#)
- pour les possesseurs d'iphone, direction l'[App Store](#)

Signal vous demande si vous l'autorisez à accéder à vos contacts. Dans l'affirmative, il intégrera alors dans l'application tous les contacts qui ont Signal installé sur leur téléphone. L'application vous informe dès qu'un nouveau contact installe Signal. Vos contacts qui sont déjà sur Signal recevront une notification les informant que vous utilisez désormais l'application.

Une fois l'application correctement installée, choisissez un nom de profil et un avatar. C'est le nom qui apparaîtra pour vos contacts. Attention, il faut bien comprendre que vous ne pouvez utiliser Signal qu'avec les personnes qui utilisent eux-même cette application.

Une fois ceci précisé, explorer quelques minutes l'application. Faire les actions suivantes afin de se familiariser avec l'application :

- Envoyer un message écrit à un ami (et vice versa)
- Envoyer un message vocal
- Passer un appel (Dans la conversation : cliquer sur le téléphone avec un cadenas)
- Passer un appel vidéo (faire un appel, puis cliquer sur la caméra qui s'affiche lors de l'appel en cours)
- Envoyer un fichier
- Lancer une conversation de groupe (Sur l'écran d'accueil, qui affiche toutes les conversations, cliquer sur les trois points en haut à droite, puis Nouveau groupe)

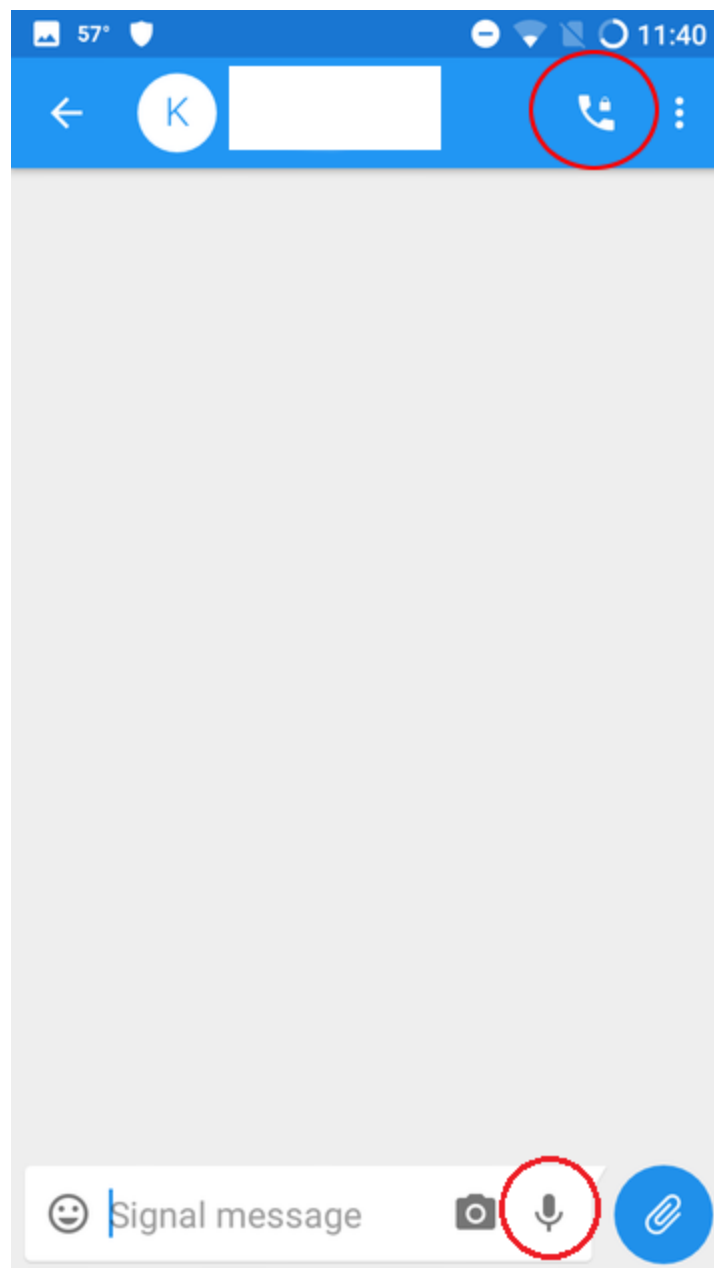


Give your inbox something to write home about. Get started by messaging a friend.

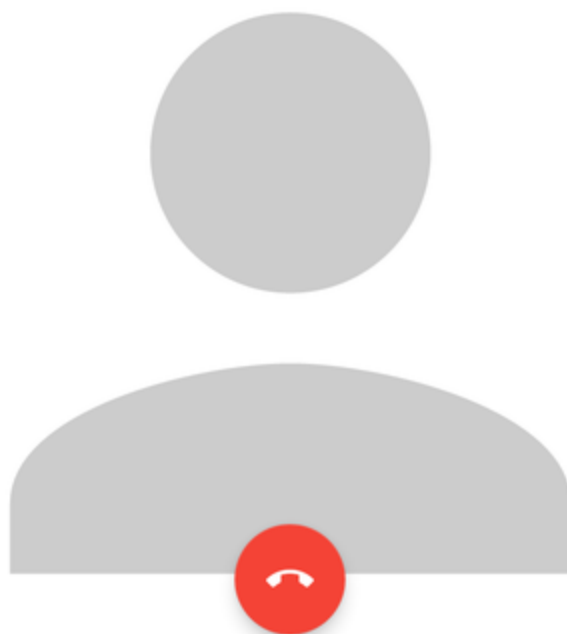
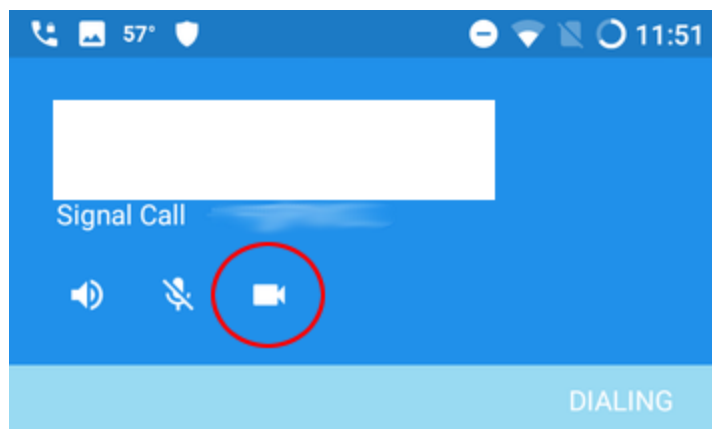


Pour démarrer une conversation, cliquez sur le stylo puis sélectionnez un contact

Toutes ces étapes seront très instinctives, car l'application ressemble à toute autre application de communication.



Pour lancer un appel vocal ou laisser un message vocal



Pour lancer un appel vidéo, cliquez la caméra

Il existe aussi la possibilité d'envoyer des messages éphémères qui s'effacent après lecture :

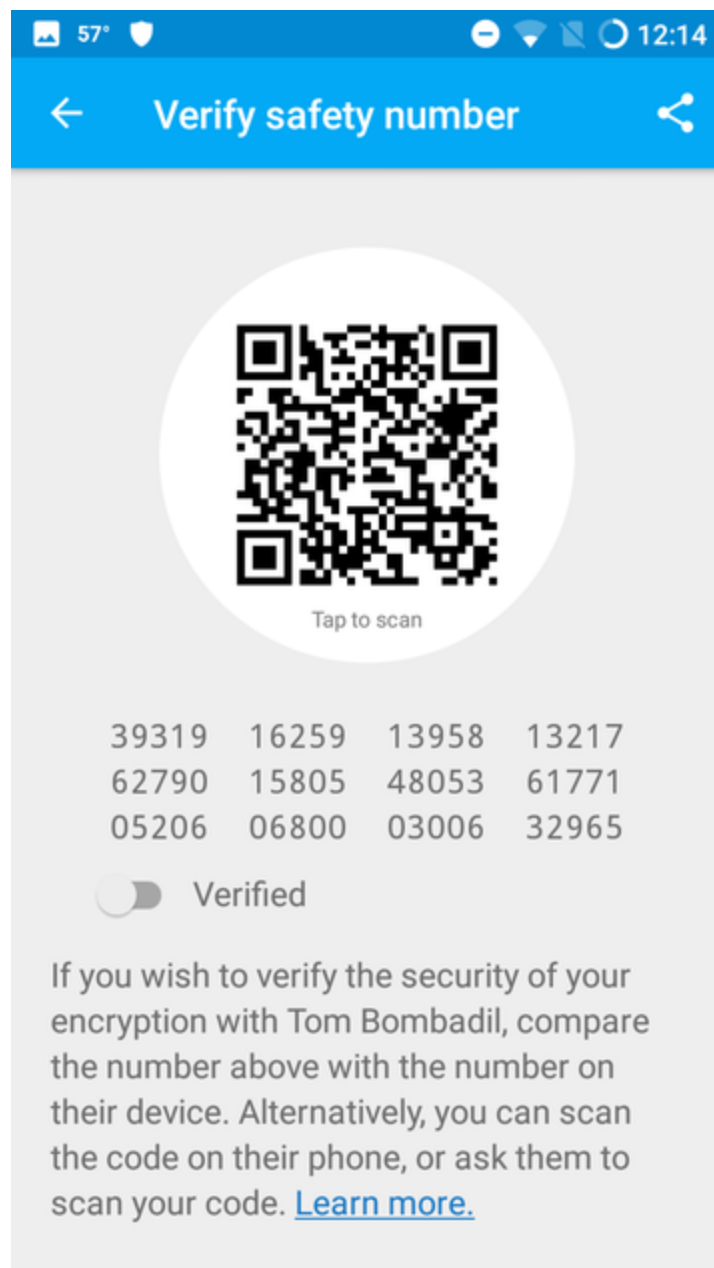
- Sur Android : Paramètres (les trois petits points en haut à gauche de l'écran) > Messages éphémères > Sélectionner la durée. Si vous sélectionnez 5 secondes, une fois que le destinataire du message lit le message, celui-ci disparaît 5 secondes après. (Va de 5 secondes à une semaine).
- Sur Iphone : Cliquer sur le numéro de la personne, dans la conversation > Message éphémère > Choisir le temps

Si vous souhaitez ajouter une sécurité supplémentaire, vous pouvez "authentifier

deux téléphones". Chaque téléphone a un QR Code unique, que vous pouvez scanner. Signal enregistre que ce numéro et ce téléphone correspondent à ce QR Code.

Vous pouvez authentifier le téléphone d'un ami. Cette fonctionnalité – avancée – sert à s'assurer que lorsque vous discutez avec quelqu'un sur Signal, l'interlocuteur au bout du fil est bien la personne qu'il prétend être. C'est un peu comme une carte d'identité pour chaque utilisateur de Signal. Celui-ci vous la montre, vous l'enregistrez alors dans votre téléphone, et si un jour votre interlocuteur change de téléphone ou si quelqu'un usurpe son numéro pour l'utiliser sur un autre téléphone, Signal vous enverra un avertissement lors de la conversation.

- Sur Android : dans la conversation > Paramètres (les trois petits points en haut à gauche de l'écran) > Paramètres de la conversations > Afficher le numéro de sécurité.
- Sur Iphone : Cliquer sur le nom et numéro du contact dans la conversation > Afficher le numéro de sécurité.



Pour authentifier un téléphone

Vous avez découvert les fonctionnalités principales de l'application Signal, si vous souhaitez approfondir le sujet nous vous conseillons de parcourir [le guide pratique complet](#) édité par Signal.