TOOL – COMMUNICATING WITH SIGNAL

COMMUNICATION & COLLABORATION > 2.1 INTERACTING THROUGH DIGITAL TECHNOLOGIES

TARGET GROUP	AGE GROUP	PROFICIENCY LEVEL	FORMAT	COPYRIGHT	LANGUAGE
Facilitators	N/A	Level 1	Preparatory guide	Creative Commons (BY-SA)	English, French

This document contains background information for facilitators before they run the workshop with participants. It gives an understanding of how to use how to use the communication app known as Signal.

General Objective	Skillset building
Preparation time for facilitator	less than 1 hour
Competence area	2 - Communication & collaboration
Name of author	Nothing 2hide
Resource originally created in	French

WORKSHOP DIRECTIONS

1 Introduction to communication encryption

Your communications contain a wealth of information. This can be used for a variety of particular reasons, for example as part of a court case. However, what is more often the case, your communication apps tend to use your data for targeted advertising. This is the case for example with Gmail who have used bots to scan users' emails for years in order to produce personalised ads depending on the content of those mails. Facebook Messenger also 'offers' the ability to show targeted advertising depending on the content of your conversations.

Two people discuss what they might

have for dinner. As if by magic, an add for a local food market appears in the conversation.

For your communications, there are two things to differentiate: those that pass through a traditional mobile network (phone calls and text messages) and online exchanges using the internet (Wi-Fi, 3G, 4G, etc.).

Phone calls and text messages are easy to intercept and particularly to decrypt. Someone of malicious intent and well-equipped can listen to and read your exchanges, voice or text, in real time.

For online communication, it can be a little more difficult depending on the apps you use.

Communication apps:

- Messenger: not encrypted by default. You need to use the option 'secret conversation' to encrypt your communications end to end. End to end means that only you and your recipient can access the messages, which are encrypted on your device and decrypted when they reach your friend's phone.
- WhatsApp: conversations here are encrypted here end to end by default. Be careful though: metadata – e.g. which number called which number and for what duration – is preserved.
- Skype: also features encryption but not by default: Microsoft holds the keys for encryption and decryption and can technically access your conversation. To have a truly confidential conversation you will need to use the option 'New Private Conversation'.
- Snapchat: offers no encryption. Worse, the seemingly temporary messages can be technically recovered by the company.
- Telegram: messages on this app are not encrypted by default. You will have to activate the 'secret chat' to encrypt your communication. However, contrary to Skype, Messenger and Snapchat which use common encryption systems, Telegram uses its own that is known only by the company.

To protect your private life, one of the best apps you can use is Signal.

2 Using Signal

In an interview with the French newspaper Le Monde, Signal's creators explain that their aim was:

> that every person concerned by the preservation of their private lives would be able to use a free service. We believe that everyone has the right to communicate freely and in private.

No problem – you don't need to by an actual spy. Encrypted apps are accessible to everyone. The team at Signal assures:

> that everyone will be able to communicate securely using a means as a simple and accessible as a phone call.

Signal encrypts voice and text messages. You can call or send voice or text messages. You can also send attachments (photos, PDFs, etc.).

Now, time to use app. Let's install it:

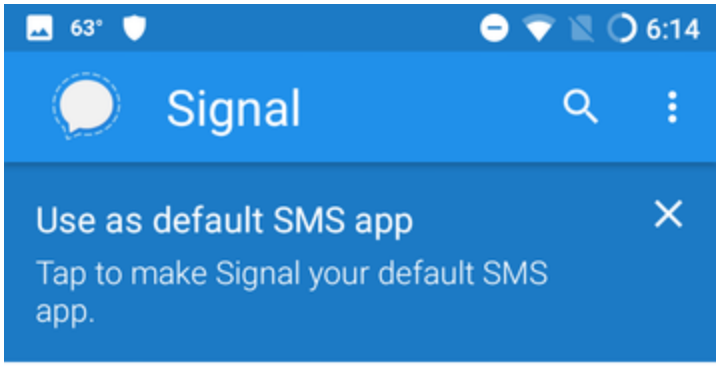
- if you have an android, use Google play
- if you have an iPhone, use App Store

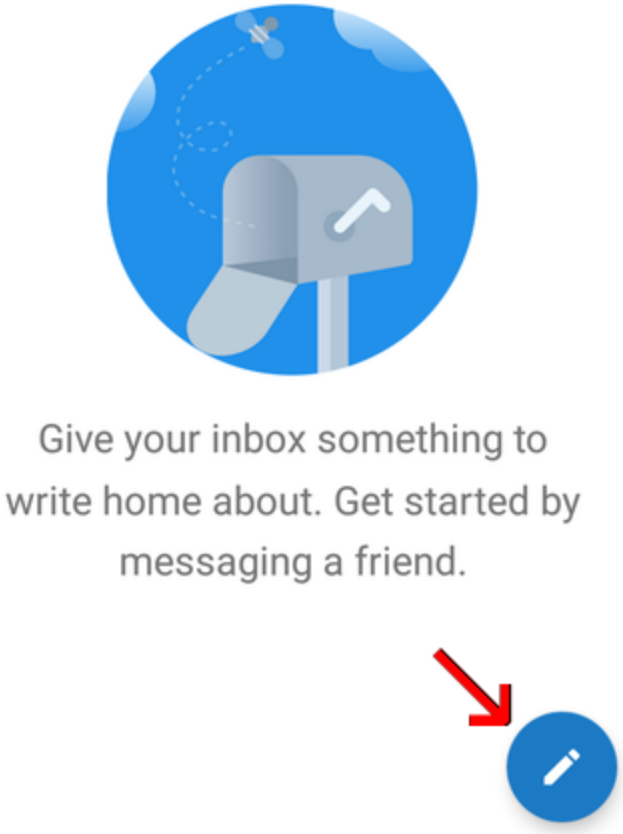
Signal asks for your authorisation to access your contacts. If you say yes, all your phone's contacts will be integrated to the app. Signal will inform you when a new contact installs it. Your contacts who are already on Signal will receive a notification informing them that you are now using an app.

Once the app is installed, choose a username and image. This is the name that will appear for your contacts. Be aware that you can only use Signal with others who have it.

Once this is done, explore the app. Try the following actions:

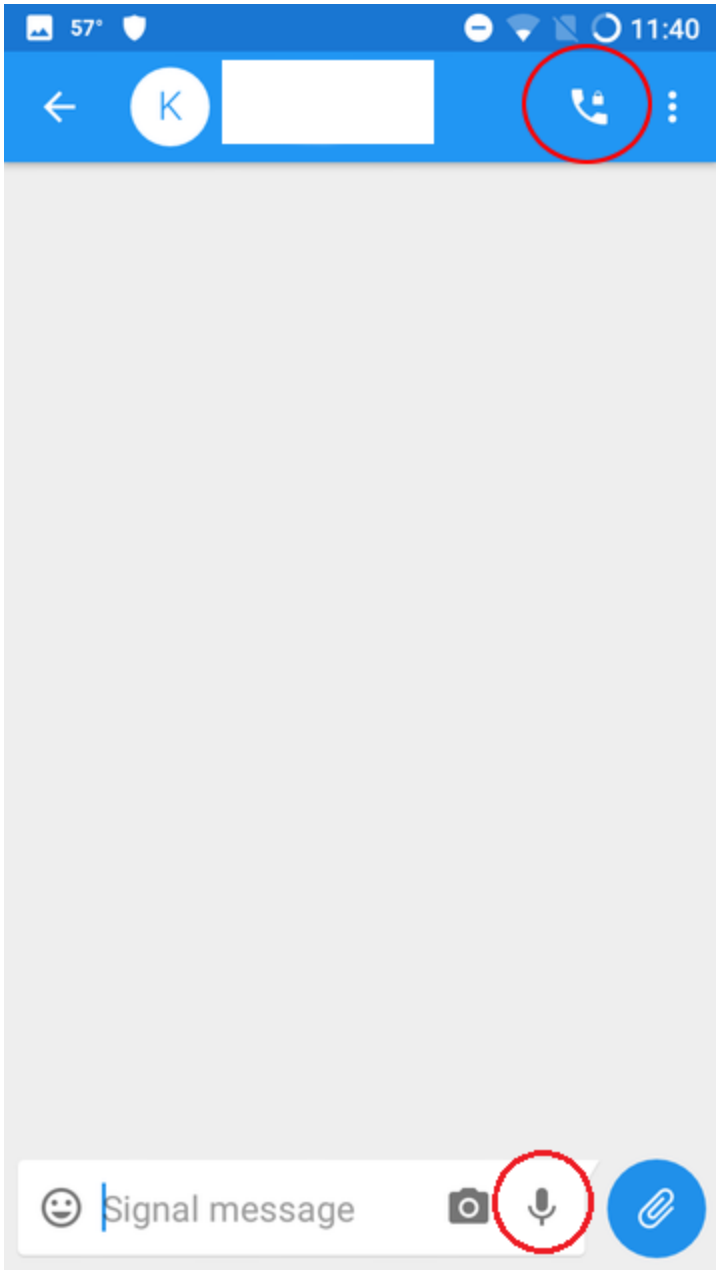
- Send a written message to a friend (and vice versa)
- Send a voice message
- Make a phone call (in the interface, tap the phone icon)
- Make a video call (make a call, then ta the camera which appears during the call)
- Send a file
- Start a group conversation (on the home screen, where all conversations are displayed, tap the three vertically arranged dots on the top right, then 'New group'.



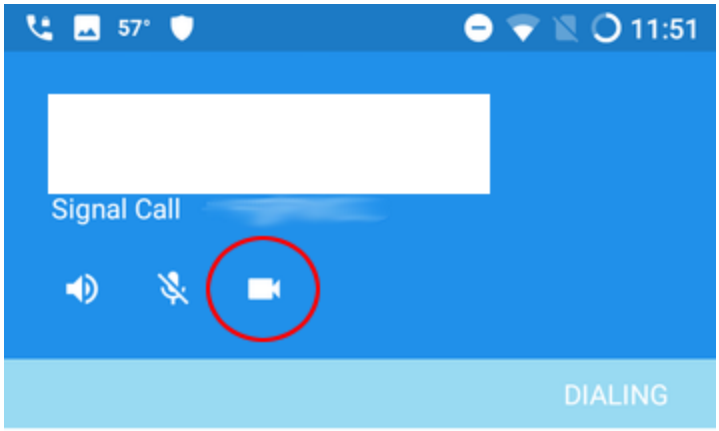


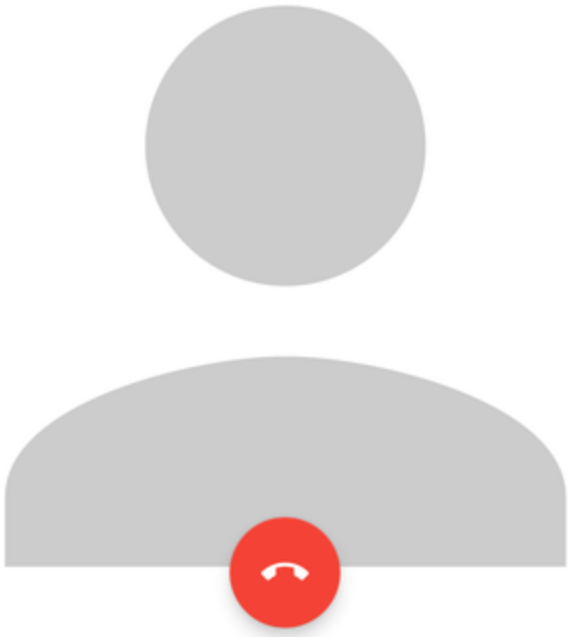
To start a conversation, click on the pencil icon the choose a contact

Each of these steps will be quite instinctive, since the application is quite like other popular messenger apps.



To start a phone call or leave a voice message





To start a video call, click the camera

You can also send temporary messages which delete themselves after they are read:

- On Android: settings (the three dots on the top left of the screen) > Disappearing messages > choose the duration. If you select 5 seconds, once your recipient read the message, it will delete itself 5 seconds later. You can choose from 5 seconds to 1 week.
- On iPhone: tap on the contact's number, in the conversation > Disappearing messages > select duration

If you want to add extra security, you can use the 'safety number' feature. Each Signal conversation has a unique safety number that allows users to verify the security of their messages and calls with specific contacts. This can be identified through the use of QR codes. Each contact receives a unique QR code which can be scanned in order to compare safety numbers.

You can verify a friend's phone. This advanced feature assures users that when they exchange with a contact on Signal, the person they are communicating with is without any doubt who they claim to be. It is a little like an identity card for each Signal user. Your contact shows you theirs, you save it to your phone, and if one day they change their phone or if someone takes their number to use it for another phone, Signal will send you a notification during the conversation.

- On Android: in the conversation > settings (three dots on top left of the screen) > conversation settings > view security number.
- On iPhone: tap on the contact's name and number in the conversation > view security number

To verify a phone

You have now learned about the principal features of Signal. For more information, see the complete official guide for iOS or for Android.