How to Install Signal (beginning)

Learning Objectives

Learners will:

- Understand why groups or people may be interested in protecting their communications.
- Understand what metadata is and what data Signal collects.
- Install Signal on their phone.
- Demonstrate understanding of safety numbers by verifying their safety number with a partner or the trainer.
- Send an encrypted message to a partner or the trainer.

Prerequisites

- Audience has an understanding of end-to-end encrypted communications.
- Group can dedicate at least 1.5 hours to the session.

Depending on the size of the group, it's best to break up into smaller groups so you have one trainer or helper to every five participants. This way, you can answer questions and check to ensure everyone has properly installed Signal, verified their safety numbers, and sent an end-to-end encrypted message.

Ratio

Instructor: Learners
1:5 (One instructor to five students)

GOTCHAS AND PROBLEMS YOU MIGHT HIT

- Sometimes it takes time for a new contact to display in someone's Signal contact list, or they will have to refresh their list of signal contacts. Keep this in mind during your training. Consider having participants exchange numbers

with their partners earlier in the training.

- As with other tool installations, you may encounter connectivity issues. Consider setting up your own wireless system for others to tether to your device, in case the connection fails.

- Some participants may not feel comfortable sharing their phone number with others during this training, or may not feel comfortable using their personal phone number for Signal. The following articles can help you prepare for this kind of situation:
    - How to Use Signal Without Giving Out Your Phone Number by Jillian York
    - Using Signal Without Giving Your Phone Number by Martin Shelton
    - How to Use Signal Without Giving Your Phone Number by Micah Lee

- Signal protects your communications, but will not protect against other reading your texts or malware retrieving your messages. It's important to point out that Signal is not a panacea against all threats.

- Sometimes people will not have enough storage space left to install Signal. You may want to have people think about which apps are unnecessary before coming to the session.

Recommended Reading

- How to: Use Signal on iOS
- How to: Use Signal on Android
- Different Types of Encryption

Lesson Content

ICE BREAKER

Ask, "Did you ever use a secret language or codes as a kid to pass messages to your friends?"

Invite learners to describe what they did. Some examples could include Pig Latin or other kinds of codes, lemon juice ink or other kinds of “invisible” writing, etc.

WARMUP

Ask, "Why might someone want to protect their digital communications? What groups or people may be interested in protecting their communications from telephone providers, law enforcement, governments, etc.?"

Answers may include:

- Journalists
- Lawyers
- Human rights defenders, activists, and dissidents
- LGBTQ youth
- Academic researchers
- People traveling overseas (Signal uses data, not minutes)

Follow up with, "How can someone better protect their digital communications?"

Allow for ideas, and then lead the discussion towards end-to-end encrypted communications. Participants should have presumably reviewed that module/topic already. This should be a refresher.

KNOWLEDGE SHARE: Introducing Signal

Introduce the topic with, "An example of a tool that allows for end-to-end encrypted conversation is Signal. We’re going to learn how to download the app on your phone today."

Take this opportunity to review learning objectives with your audience, and then share the following points:

- Signal is a free and open source mobile app developed by Open Whisper Systems that employs end-to-end encryption on iOS, Android, and desktop.
- Signal uses telephone numbers as contacts and can send end-to-end encrypted phone calls, texts, video calls, and files between Signal users using

data or wi-fi. This means Signal users don't incur SMS and MMS fees, but both parties to the conversation must have Internet access on their mobile devices.

- If you download it and allow access to your contacts, you may be surprised to find some of your friends already using it.
- It's more secure than making regular phone calls and sending standard SMS messages.
- If you're in a country that monitors people's communications, though, they may be looking for Signal traffic. Do your research!
- Signal's privacy policy is short and concise. Unlike WhatsApp, Signal doesn't store any message metadata. (Pause here to define metadata.) The closest piece of information to metadata that the Signal server stores is the last time each user connected to the server, and the precision of this information is reduced to the day, rather than the hour, minute, and second.

Ask your audience if there are any questions before moving on.

INSTALL

1. Break the group up into small groups (maximum five people in each) and tell them they'll be doing a step-by-step install. Where possible, pair Android users with other Android users and iOS users with other iOS users.

Tip: Use install cards. Give users a green card, a yellow card, and a red card. They should display the green card when they've completed a step and no help is needed, the yellow card if they're working on a step, and the red card if they're stuck and have questions.

2. Prompt learners to visit either the Google or Apple App Store, search for "Signal," and download the app.

Pause here to ensure everyone has successfully downloaded the app.

3. See How to: Use Signal on iOS and How to: Use Signal on Android to continue with the app set-up. Pause after each step to ensure everyone has completed each step. Stop when you get to the "Using Signal" section.

KNOWLEDGE SHARE: Fingerprints/Safety Numbers

Introduce the topic with, "Before we try to send a message through the app, we need to verify the identity of the person with whom we're communicating."

Remind students of the "verifying fingerprints" section in end-to-end encrypted communications module/topic. If necessary, review the concept with an activity or slides.

End-to-end encrypted applications often have ways to verify your friend's identity. As a reminder, a fingerprint is a short mathematical representation of your encryption keys that looks like gibberish. You can use fingerprints to verify that you are communicating with the intended person, and that your messages aren't tampered with.

Signal uses something a little different called a "safety number." In Signal's case, the safety number is a mathematical representation of the conversation session between you and your recipient (half your unique public key, half their unique public key). Each half of the safety number is persistent until that person reinstalls Signal (thus creating a new cryptographic identity).

The safety number is a powerful way to check the security of your communication with a friend, and to protect against something called a "man-in-the-middle" or "machine-in-the-middle" attack. However, you should know that safety numbers can change for innocent reasons as well, like your contact getting a new phone, reinstalling Signal, or configuring Signal to a new device.

If you know you are getting a new phone, you can notify your friends that your safety number with them will change. Some ways you can do this are by sending a Signal message before getting your new phone, posting a general announcement on an HTTPS-encrypted site, telling them in person, and so on. That way, they know not to be surprised that your device information has changed.

Pause here for a break before doing the next activity. Tell learners they'll be verifying their safety number with a partner (or the trainer) after the break. Make yourself available for questions.

ACTIVITY: Verifying Safety Numbers

Have people find a partner. Tell them they will be exchanging phone numbers with this partner. The trainer or helpers should be available to partner with those who feel uncomfortable giving their phone number to a stranger. Make your phone number or burner phone number available on the board or projector.

Tip: Use install cards.

1. Have students exchange phone numbers with their partners. They should do this by creating a new contact in their phone and entering their partner's number into their contact list.

Pause and check to ensure everyone has successfully added a contact.

2. See instructions under "How to Verify Your Contacts" in the How to: Use Signal on iOS and How to: Use Signal on Android guides to continue with this activity. Pause after each step to ensure everyone has completed each step. Stop when you get to the "Using Signal" section.

For advanced learners: Learners who have easily exchanged their safety number with one other person should find others in the room to exchange a safety number with while the trainer helps those who are having difficulty.

3. Once people have successfully checked their safety number with someone else, have them display their green signal card.

4. Bring the group back together once everyone has completed the task.

Ask your audience if there are any questions before moving on.

ACTIVITY: Sending an End-to-End Encrypted Message

Introduce this next activity with, "Now that you've verified the identity of the person you're communicating with, you're ready to send an end-to-end encrypted message." Have learners find their partners. (And remember: in some cases, the partner may be the trainer or the helper.)

Tip: Use install cards and reference the "How to Send an Encrypted Message" section of the Signal guides.

1. Have everyone open Signal on their phone and tap the compose icon in the upper-right corner of the screen.

Pause to ensure everyone knows where this is located on their phone.

2. Walk through the step-by-step instructions in "How to Send an Encrypted Message" section on the Signal guides.

3. When students have successfully sent an encrypted message to their partner, have them display their green signal card.

OPTIONAL CLOSING ACTIVITY

Write down a list of three contacts whom you will help to install Signal after this training.

FOR THOSE IN THE AUDIENCE WHO WANT TO LEARN MORE

All of the material covered today came from EFF's Surveillance Self-Defense Guide. Related resources to check out include:

- How to: Use Signal on iOS
- How to: Use Signal on Android
- The glossary
- Signal support center

ANTICIPATED QUESTIONS & ANSWERS

Q: What if I'm uncomfortable granting Signal access to my contacts?
A: Signal uses a cool technique called private contact discovery to make it possible for you to determine whether the contacts in your address book are Signal users *without revealing your contacts to the Signal service*. The details get a bit nitty-gritty, but people who'd like to learn more can check out Signal's blog post about the technique.

Q: If Signal is so secure, why does it log all my messages?
A: Signal has a feature called "disappearing messages" which ensures that messages will be removed from your device and the device of your contact some chosen amount of time after they are seen. To enable "disappearing messages" for a conversation, open the screen where you are able to message your contact. From this screen, tap the name of the contact at the top of the screen, then tap the slider next to "Disappearing Messages."

Q: What about WhatsApp? All my friends use it.
A: We don't currently recommend WhatsApp for secure communications, but understand quite a lot of people use the app—especially internationally. Check out our WhatsApp guides for Android and iOS.

Q: Will I be targeted if someone knows I have an end-to-end encryption application installed on my phone?
A: In some countries, using Signal or other end-to-end encrypted messengers can indeed be a red flag to law enforcement, government authorities, or others monitoring at a network level. If this is a concern for you, then Signal might not be the right choice.

Q: How do I get my friends to use this app? None of them seem concerned with protecting their communications—they say they have nothing to hide.
A: Some ideas include asking if you can install the app for your friends, telling them that Signal is the best (or only!) way to contact you, and mentioning that Signal is free and works internationally.