CERT-EU Security Guidance 22-002

Hardening Signal

CERT-EU Team
ver. **1.0**
03-03-2022

TLP:WHITE | LIMITED DISCLOSURE
TLP:WHITE information may be distributed freely.

https://t.me/learningnets

Contents

https://t.me/learningnets

History:

- *03/03/2022 - v1.0 - Initial publication.*

1 Introduction

Signal is a well-known, secure, encrypted instant messaging service developed by the non-profit Signal Technology Foundation and Signal Messenger LLC. It uses standard cellular telephone numbers as identifiers and all communications between Signal users are secured with end-to-end encryption.

Staff of public and private organisations, including senior management, may be using Signal sometimes to quickly coordinate and exchange information on work-related matters. Signal groups may also have been set up for business continuity reasons in case corporate instant messaging tools become unavailable.

The following document provides clear and pragmatic recommendations for hardening the configuration of Signal apps. If you have suggestions that could help improve it, contact us at services@cert.europa.eu. We always appreciate constructive feedback.

2 Scope and audience

This document provides guidance for hardening Signal apps.

The audience of this document are all staff using Signal for work-related matters.

3 Hardening recommendations

3.1 Use the official websites and stores to download the Signal apps

Only download the Signal apps from the official websites and stores:

- Apple iOS devices.
- Android devices.
- Desktop applications.

3.2 Use auto-update or regularly update your apps

Update regularly your applications and choose auto-update whenever possible:

- On iOS devices, go to `Settings > App Store` and check `App Updates`. Refer also to Apple's How to manually update apps on your Apple device.

https://t.me/learningnets

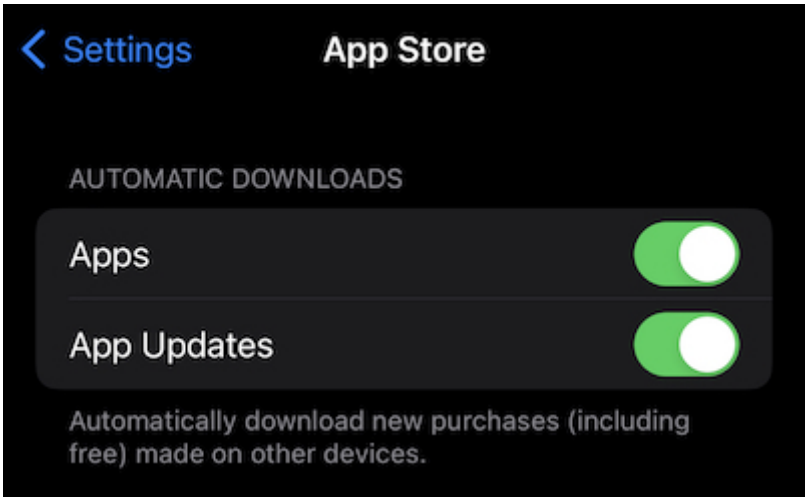

Figure 1: Signal iOS Updates

- On Android devices, refer to Google's How to update the Play Store & apps on Android.
- On Desktop applications go to `Preferences > General` and check `Automatically download updates`.

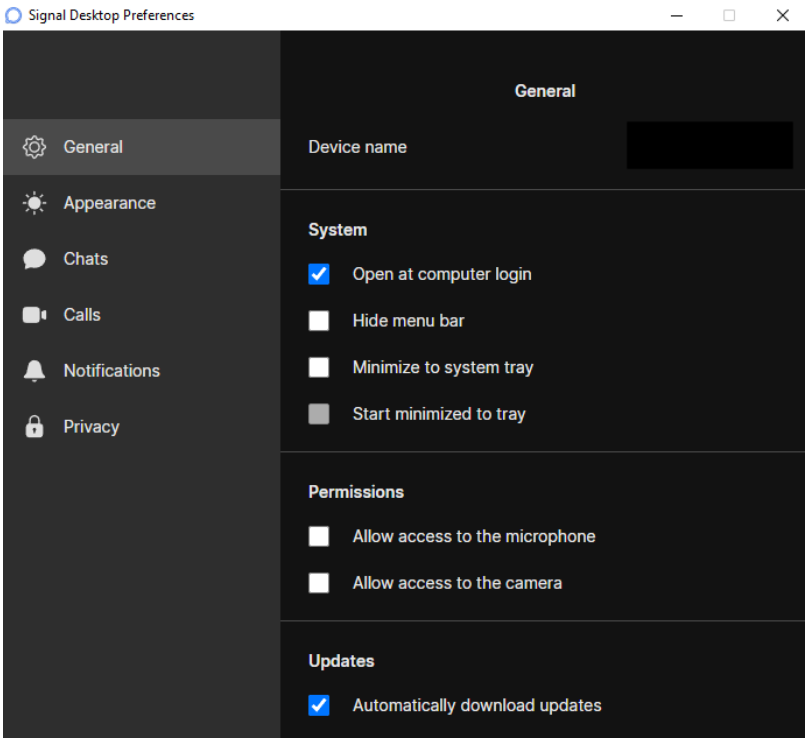

Figure 2: Desktop Automatic Updates

3.3 Customise your profile

We recommend you use your real name and provide a short bio. You may also customise your picture's profile to your liking, using preferably a real picture:

1. Tap your profile icon/picture on the top left corner of the application, then select `Settings`.
2. Select the first area where your current profile icon/picture is and customise the picture/bio.

https://t.me/learningnets

3.4 Verify the identify of your contacts

Do not accept contact requests from numbers that are not registered in your contacts without proper verification.

If a person contacts you for the first time on Signal, using a name that should be known to you but for which you don't have a corresponding phone number in your contact list, or if the person is not already a member of one of your trusted Signal groups:

1. Note down their phone number.
2. Contact the person they pretend to be using **another** trusted means of communication (e.g. by contacting them using your corporate chat platform or by sending them an email using their corporate email address) and ask them if they have tried to initiate a conversation with you on Signal. Provide the phone number you noted down in the first step.
3. If they confirm, you may accept the conversation.
4. If they refute, block the impersonator on Signal and **report this immediately** to your security officers.

You may also want to verify the identity of your contacts by checking their Safety Number:

1. For each contact, select the conversation you have with them, then tap on their profile icon/picture and select `View Safety Number`.
2. Screeshot the QR code or note down the safety number and use another trusted means of communication (e.g. by contacting them using your corporate chat platform or by sending them an email using their corporate email address) to ask them to confirm the number. You can also use the "sharing option" of your device to send them the safety number on your corporate chat platform or by email.
3. Once they confirm the number matches on their side, you can make the contact "trusted" by clicking on `Mark as verified` in Signal.
4. If the contact uses a device other than the one you just approved, Signal will tell you so. In this case, perform the previous steps again to reverify their safety number.

https://t.me/learningnets

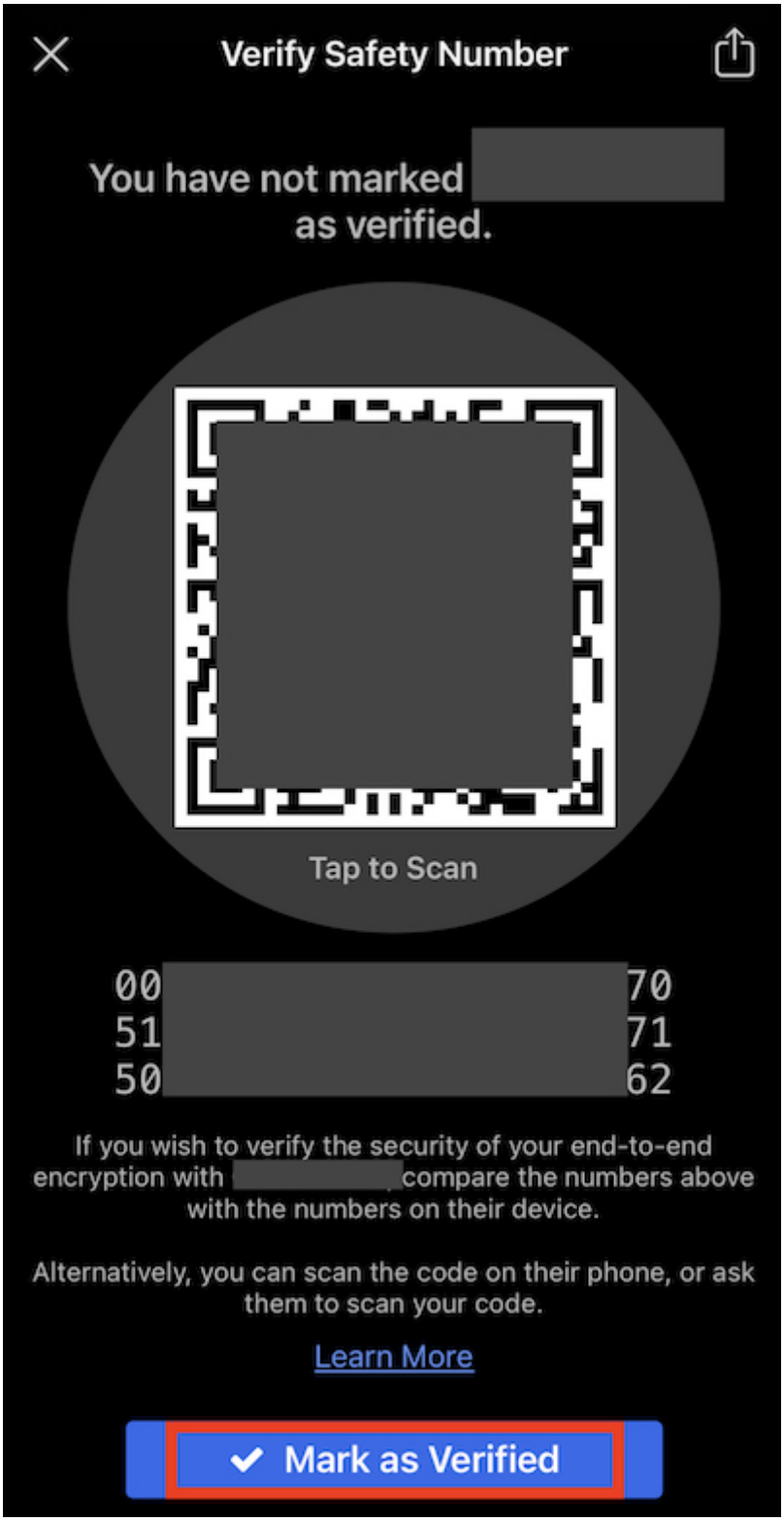

Figure 3: Safety Number

3.5 Enable Registration Lock

Your Signal account is linked to your phone number. If someone gets access to it, they can impersonate you, using for example a SIM swapping attack. To avoid this, you must activate Registration Lock:

https://t.me/learningnets

1. Tap your profile icon/picture on the top left corner of the application, then select `Settings`.
2. Select `Account` then activate `Registration Lock`.

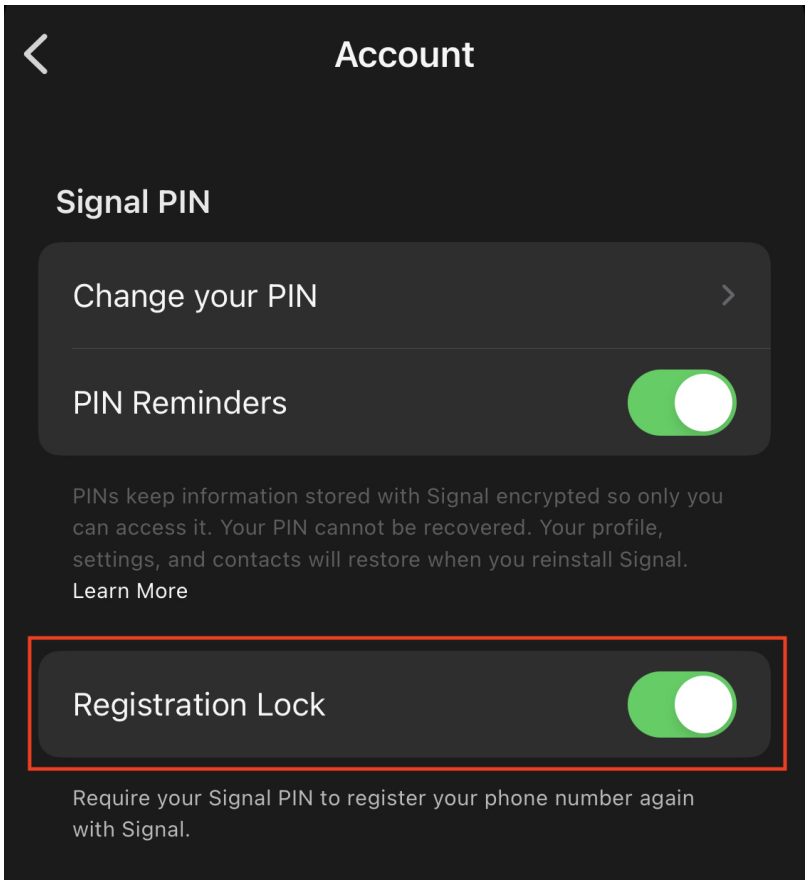

Figure 4: Registration Lock

When you activate this option, Signal will ask you to create a PIN that will be required for account registration, in addition to standard SMS-based verification. **We strongly encourage you to choose an alphanumeric PIN** and to record it in a safe, secure place (e.g. your corporate password manager).

3.6 Make sure your account is only synchronised on devices you trust

Only synchronise your account on secured and trusted devices. If one device is compromised, this will allow the attackers to see all the content of your conversations:

1. Tap your profile icon/picture on the top left corner of the application, then select `Settings`.
2. Select `Linked Devices`.
3. Check that you recognise all the devices listed there if any.
4. If there is a suspicious device in the list, **report it immediately** to your security officers providing:
   a. its name as it appears in the list,
   b. the date at which it was linked (`Linked dd/mm/yyyy`),
   c. the last active date (`Last active dd/mm/yyyy`).

https://t.me/learningnets

5. Then select `Edit` from the right top corner of the app, press the “deletion” sign on the left-hand side of the suspicious device and select `Unlink`.

3.7 Activate the screen lock

Activate the screen lock:

1. Tap your profile icon/picture on the top left corner of the application, then select `Settings`.
2. Select `Privacy` and toggle `Screen Lock` under App Security.
3. Choose a sensible timeout (e.g. 5 minutes).

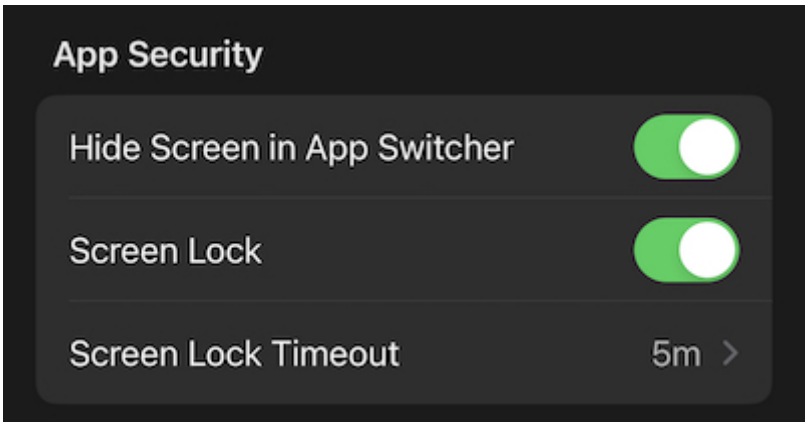

Figure 5: Screen Lock

3.8 Enable notification privacy

Even when your device is locked, anyone could pick it up and read messages and sender names from your lock screen. This is particularly easy during meetings with external parties.

We recommend that you configure Signal in a way that only the sender’s name is displayed when your device is locked:

1. Tap your profile icon/picture on the top left corner of the application, then select `Settings`.
2. Select `Notifications` then `Show` under Notification Content.
3. Select `Name only`.

You can also prevent the sender’s name from being displayed altogether by selecting `No Name or Content` instead of `Name only` in the last step.

https://t.me/learningnets

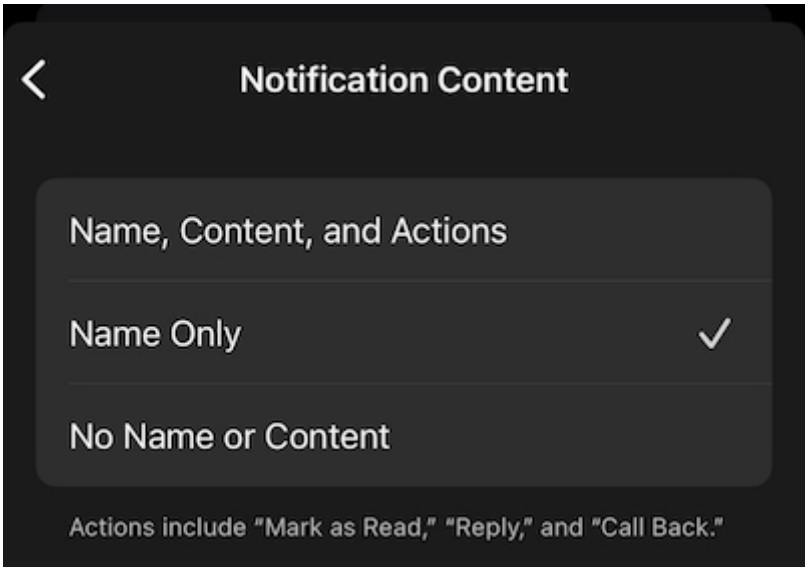

Figure 6: Notifications

3.9 Make your messages disappear

Use Signal's "disappearing messages" feature to remove messages from a conversation automatically after a certain time:

1. Tap your profile icon/picture on the top left corner of the application, then select `Settings`.
2. Select `Privacy` then `Default Timer for New Chats` under Disappearing Messages.
3. Choose a sensible default timer (e.g. 1 week).

Disappearing Messages - Global

On existing conversations:

1. Tap on the profile icon/picture of your correspondent/group.
2. Select `Disappearing Messages`.
3. Choose a sensible default timer (e.g. 1 week).

https://t.me/learningnets

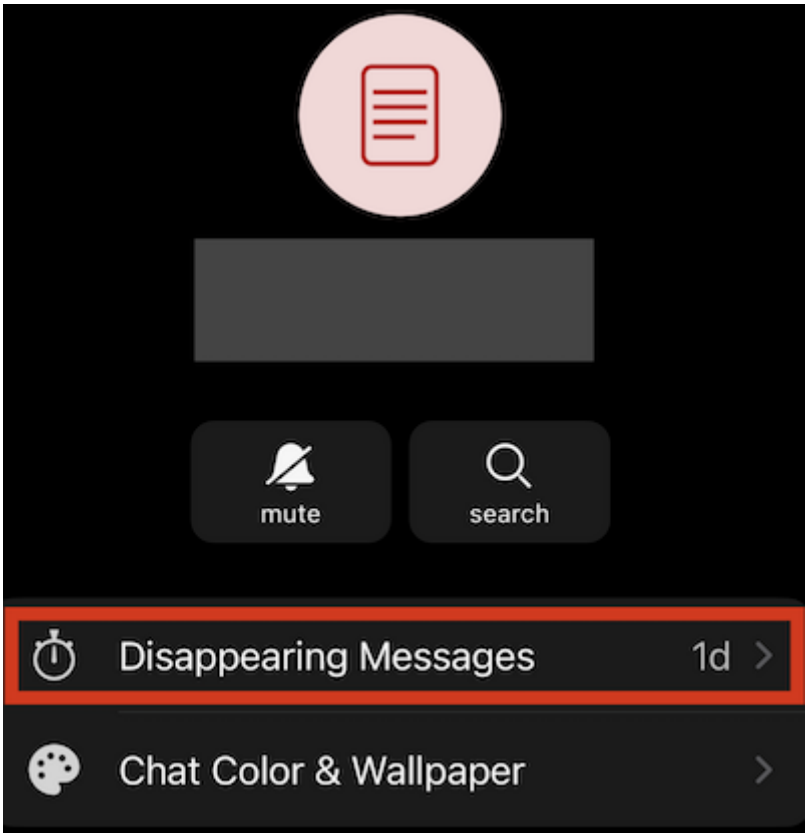

Figure 7: Disappearing Messages - Each Conversation

3.10 Reboot your phone regularly

Reboot your phone at least once a day. While this will not prevent your device from being compromised, a reboot would get rid of non-persistent malicious implants that may have been surreptitiously installed on it.

4 References

- Signal Official Website

TLP Definition

TLP	Disclosure	Message
RED	Not for disclosure, restricted to participants only.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed.
AMBER	Limited disclosure, restricted to participants' organisations.	Recipients may share TLP:AMBER information only with members of their own organisation.
GREEN	Limited disclosure, restricted to the community.	Subject to standard copyright rules, TLP:GREEN information may be distributed with peers and partner organisations within their sector or community, but not via publicly accessible channels.
WHITE	Disclosure is not limited.	TLP:WHITE information may be distributed freely.

https://t.me/learningnets