Martin
Roth
Initiative

Martin Roth-Initiative: Secure Communication Guide [external]

The Martin Roth-Initiative (MRI) and its partners are working with people at risk that faces different forms of threats, repression and/or surveillance. Therefore it is important that all involved actors take measures to secure (as much as possible) communication in order not to create additional risk for the supported persons.

The purpose of this Secure Communication Guide is to assist users to minimize the risk and consequences of communication being intercepted ("listened to").

This Secure Communication Guide outlines two steps to improve the security of communication:

1. Basic analysis of communication risks
2. Tools and good practices for secure digital communication

Following this guide will NOT provide 100% security for the users nor will it cover all processes of critical communication. But it will support everybody involved to take conscious decisions to improve their security for their sensitive communication. By using some of the below mentioned tools you can increase security and make it more complicated/costly for the aggressors to access and monitor the communication.

A non-encrypted e-mail or phone call is like a postcard. It can be read by almost anyone who intercepts it. It does not need much resources or technical knowledge to intercept e-mails and phone calls.

1. BASIC ANALYSIS OF COMMUNICATION RISKS

- Check how you assess your own risk of their digital and phone communication being surveilled. Recommendation on risk assessment you can get in the manuals named below
- Check, if it would be dangerous for you and your organization, if your interactions with MRI (contact, communication, exchange of docs, money transfer,…) would get known to your adversaries
- Check, if there are cases of persecution due to use of secure and encrypted apps in your region or country (like Wire Messenger in Bahrain) (using local

knowledge or use online resources like:
https://www.privacyinternational.org/type-resource/state-privacy)

The objective is to balance direct secure communication with secure apps and channels versus raising suspicion by adversary.

	Optional steps including third parties	**Digital communication steps**
For all steps including third parties: Establish secure communication channels with these first (checking if assessment steps 1+2 below also apply for these!), then extend through these secure channels if necessary.		
1 - Digital and phone communication is actively surveilled	Use in-person-meetings via third parties (establish secure communication channels with and through these)	Use secure communication channels like described below. Don't use general channels like Facebook, email, phone, SMS, Skype
2 - Secure apps are illegal or under surveillance or persecution	If possible, use in-person-meetings or channels via third parties	If 3 (Direct contact with MRI is dangerous) does not apply, you can use Whatsapp as an partially secure alternative to digitally more secure communication apps
3 - Direct contact with MRI could be dangerous	Use channels via other contacts (establish secure communication channels with and through these channels first)	If digital direct communication is necessary, use anonymization tools like TOR and TAILS (only if these are not illegal or under surveillance !) on both sides

Due to the at risk target group you should assume surveillance of communication even if you could not confirm it in your risk assessment.

2. TOOLS AND GOOD PRACTICES FOR SECURE DIGITAL COMMUNICATION

TOOLS

The following tools are safer to use (then non encrypted e-mail, chat and phone), as long as using secure or encrypted apps and tools would not be raising suspicion or creating evidence for persecution.
https://www.securemessagingapps.com provides a detailed comparison of different messengers, relating to their security.

Use case needed - generic	Tool	Info	Links to tool and instructions
Email communication secondary: file sharing	**Protonmail**	Encrypted Email - Encryption is only automatic between Protonmail-users (for communication with PGP-GPG-users this can be enabled), but can also be enabled to non-protonmail addresses - Works on phone (own apps for iOS + Android) and computer (browser based for free accounts, desktop apps for Mac OS + Windows) - Be aware if you not enable encryption to non-protonmail and send e-mails to non-protonmail addresses the communication as easily intercepted as any other non-encrypted e-mail	https://protonmail.com/
Voice (or video) conversations secondary: chat, using internal pad for note taking	**Jitsi Meet**	Fully encrypted, 100% open source video / audio / chat conferencing - one-time conversations (no saving of communications after leaving the secure room) - easy to access via link, no installation necessary - needs browser (Chrome / Firefox / Safari) on computer - easier use on phones via specific iOS / Android apps - option of hosting own installation on server	https://meet.jit.si (be aware that in the moment the most secure way of using Jitsi Meet is by hosting it on your own servers)
Messaging secondary: voice calls (2 participants), file sharing	**Signal messenger**	End-to-end encrypted messaging and call app for iOS / Android. Keeps hardly any logs. Open source. - Desktop version needs phone for registration	https://signal.org/ https://securityinabox.org/en/guide/signal/android/ https://ssd.eff.org

		- Installation and use is as easy as whatsapp	/en/module/how-use-signal-android https://ssd.eff.org/en/module/how-use-signal-ios

Use case needed - generic	**Tool**	**Info**	**Links to tool and instructions**
Messaging secondary: chat, voice/video calls (up to 10 participants, file sharing	**Wire messenger**	End-to-end encrypted messaging and call app for iOS / Android. Keeps some logs. Open source. - Anonymous registration possible with email-addresses - Two-three parallel accounts possible on one device - Team versions available	https://wire.com/en/

GOOD PRACTICES

Make sure your operating system (Mac OS, Windows, Linux, Android, iOS, ...) is up-to-date, and that security updates are installed automatically. (For further information about safe use of smart phones and computers, check Security in a Box or the EFF-Surveillance Self Defence Guide which you find in the resources list.
Make sure your browser (Firefox, Chrome, Safari, ...) is up-to-date, and that security updates are installed automatically.

When dealing with attachments:

- Check with sender over separate channel
- Examine the URL of the attachments (hover over link, longpress link)

Don't open links or attachments without checking back over a different channel with the sender. Make sure the link destination is what you would expect (shown in the bottom left of mail applications when hovering the mouse cursor over the link, or by long pressing the link on a mobile phone).

Use plain text messages and emails (non-html) over attached documents whenever possible!

Use good passwords. Best practice is to use a password manager like KeepassXC (for Mac OS, Windows, Linux) or KeePass DX (Android) or MiniKeepass (iOS), so you can have a strong, random, and unique password for each of your accounts.

Avoid taking photographs of documents to transfer bits of information. The picture might have other information that need not be shared/saved and the photo file might have metadata that isn't to be shared/saved

Use of messengers: Given that there could be criminalisation for using certain apps and the artist/activist might be forced to unlock their phones or computers, it is a good practice to use disappearing/time expiration of messages for transfer of extra sensitive information, like passwords and such. Also use of the messenger to just communicate and not store information. And use pin or password to lock the apps like Protonmail, Wire or Signal.

Additional Resources EN (online)

Digital security
https://securityinabox.org
https://ssd.eff.org/
https://www.digitaldefenders.org/digitalfirstaid/
https://gendersec.tacticaltech.org/wiki/index.php/Main_Page

Risk assessment
Protection International: *New Protection Manual for Human Rights Defenders* (2009) https://www.protectioninternational.org/wp-content/uploads/2012/04/Protection-Manual-3rd-Edition.pdf (page 15-43)
https://holistic-security.tacticaltech.org/chapters/explore/2-8-identifying-and-analysing-threats.html

Holistic security
https://holistic-security.tacticaltech.org/
http://integratedsecuritymanual.org/
https://capacitar.org/capacitar-emergency-kit/

Additional Resources ES (online)

Digital security
https://securityinabox.org/es/
https://ssd.eff.org/es
https://gendersec.tacticaltech.org/wiki/index.php/Main_Page

Risk assessment
Protection International: see their website

Holistic security
https://capacitar.org/capacitar-emergency-kit/

Additional Resources FR (online)

Digital security
https://securityinabox.org/fr/
https://ssd.eff.org/fr

Holistic security
https://capacitar.org/capacitar-emergency-kit/