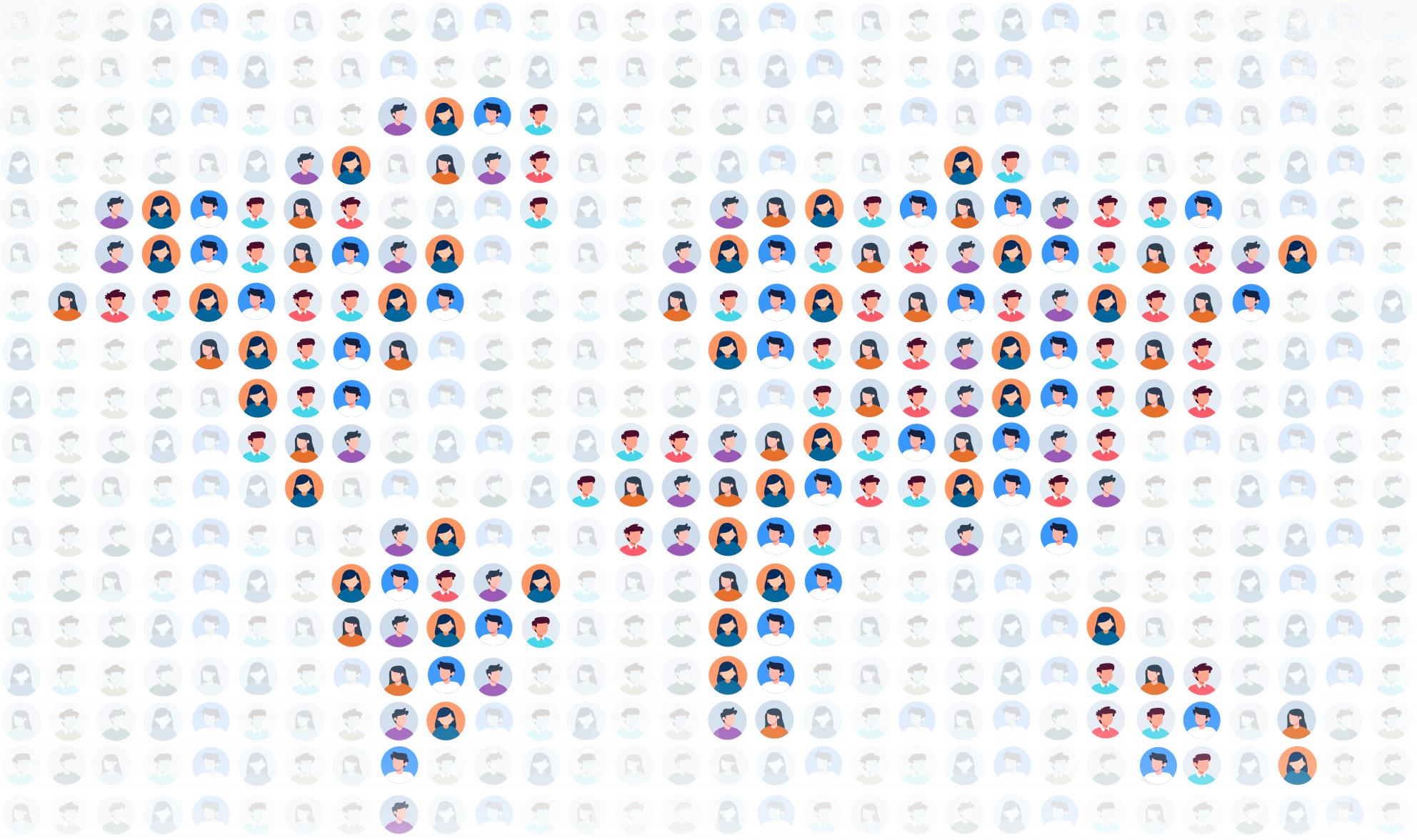


THE DIGITAL SECURITY MANUAL

A Roadmap to Online Protection

مهارات
Maharat

THE DIGITAL SECURITY MANUAL

A Roadmap to Online Protection

This manual was prepared by Maharat Foundation, with the support of UN Women and the French Embassy in Beirut.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

مهارات
Maharat

UN WOMEN

MODULE

2

SECURE COMMUNICATION:

Recommendations for encrypted messaging apps and secure email services.

Prepared by:
Digital security expert
Bahaa Nasr

Secure communication

In today's world, digital communication has become the **most common tool we use to connect** with each other. From personal chats to sensitive business communications, the rise of cyber threats has highlighted **the need for secure communication tools**. Encryption is one of the most effective ways to ensure that only intended recipients can access the information being exchanged.

Encryption is the key

When choosing a messaging app or communication service, **encryption is the most important factor** to consider. Encryption ensures that messages are **transformed into unreadable code during transmission**, making it nearly impossible for third parties to read the communication.

1

There are two main types of encryption:

Transport Layer Encryption

Protects data in transit but the **message can be decrypted by the service provide**r. This mean that the message itself is not encrypted, but it is transferred from your device to the service provider through an encrypted channel and then transferred to the intended recipient or recipients again in an encrypted channel. **This means that the service provider and sometimes hackers can read these messages.**

End-to-End Encryption (E2EE)

Ensures that only **the sender and recipient can encrypt and decrypt and read the message.** Even the service provider used to send the message cannot read its content. This mean that the messages itself is encrypted in the app on your device and sent encrypted to the receiver or receivers, where it needs to be decrypted to be read. So even **if someone manages to intercept the message, they will not be able to read it because of the encryption.**

2

Selected recommended apps and services that prioritize privacy and security:

Signal is widely regarded as one of the most secure messaging apps available. It uses **strong end-to-end encryption by default,** ensuring that only the sender and receiver can access the messages. In addition to that, Signal is **open-source,** which means the app's code is publicly available for other programmers to check its security, **enhancing its credibility and transparency.** In addition to one-on-one and group messaging, **Signal supports encrypted voice and video calls.**

Key Features:

- End-to-end encryption for all messages and calls.
- Disappearing messages feature for added privacy.
- Open-source and regularly audited for security vulnerabilities.
- Very minimal meta data collected.
- You need a mobile number to create an account, but after that you can add a username and share only your username, keeping the phone number private.

Many more features to enhance your privacy and security are available inside the app. We advise you to check the settings and adjust them according to your needs and risk profile.

2

Selected recommended apps and services that prioritize privacy and security:

WhatsApp is a **popular messaging app** that offers **end-to-end encryption for messages, calls, and media shared between users.** Although it provides strong encryption, **WhatsApp is owned by Meta (formerly Facebook), a fact that has caused information security advocates to raise privacy concerns regarding data management** (and the potential risk of Meta handing over data to governments or other stakeholders). WhatsApp is **not open source, meaning that nobody can see how exactly data is transmitted,** stored and managed which makes it difficult to check privacy and security claims made by Meta.

Key Features:

- End-to-end encryption for all communications.
- Easy-to-use interface and wide adoption.
- Supports group chats, voice, and video calls.
- Easy file sharing.

2

Selected recommended apps and services that prioritize privacy and security:

Wire is a communication app that offers end-to-end encryption for messaging, voice, and video calls. It also includes **collaboration tools such as file sharing and team chats.** Wire is **owned by a Swiss company**, is compliant with **strict data protection regulations, including GDPR**, making it suitable for businesses and organizations that require secure and private communication channels.

Key Features:

- End-to-end encryption for all communications.
- Collaboration tools and file sharing for teams.
- GDPR compliant and enterprise-ready.
- Open-source and audited.
- You can create an account without a mobile number.

2

Selected recommended apps and services that prioritize privacy and security:

Telegram offers **end to end encryption for its "Secret Chats"** only, **standard chats are only encrypted during transit**. Users need to activate this feature manually to start a "Secret Chats" every time.

Key Features:

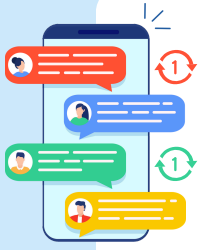
- End-to-end encryption available only in Secret Chats.
- Supports large group chats and channels.
- Auto-delete messages for enhanced privacy.

3 Recommendations

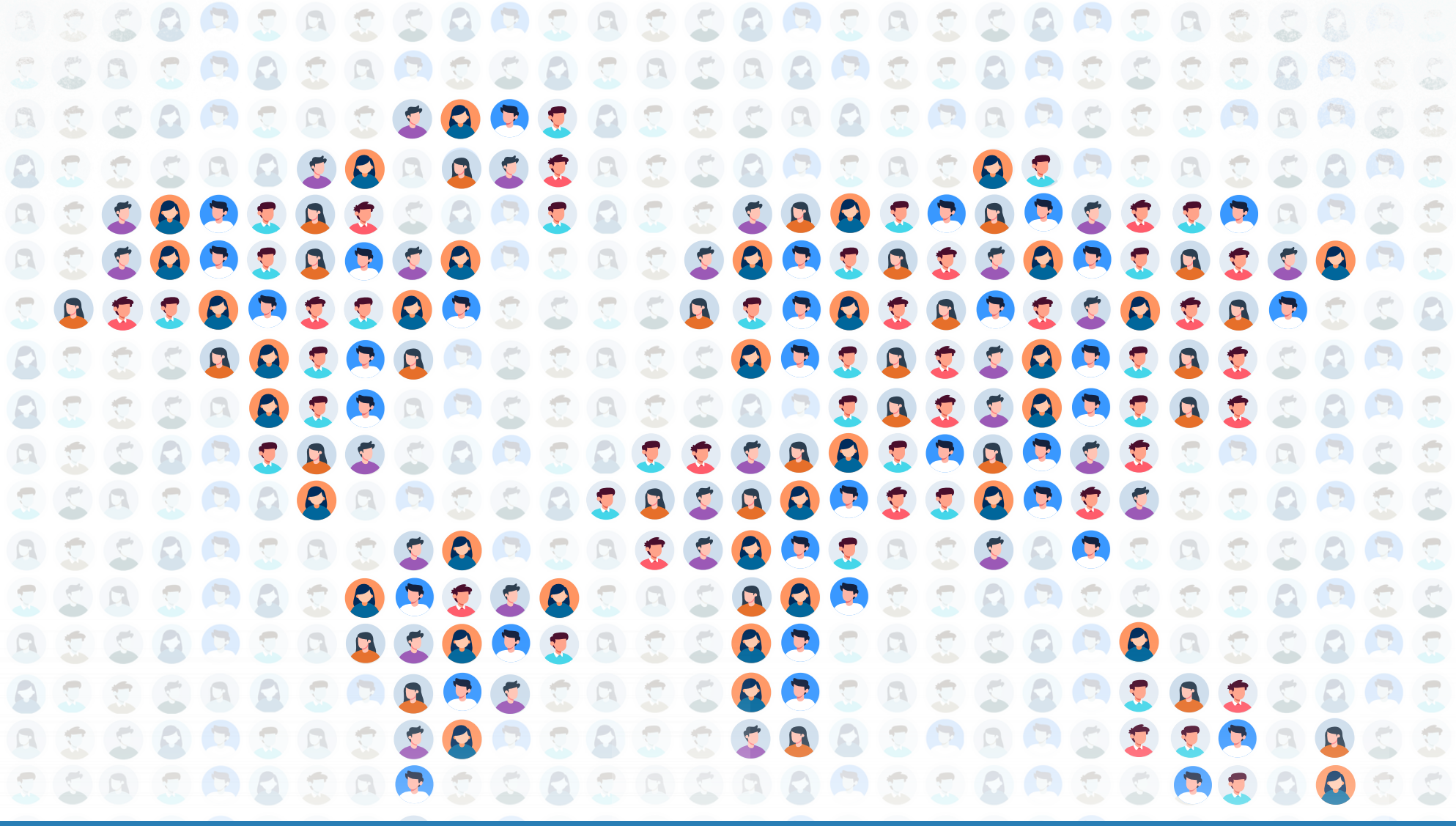
Using a secure communication app is an essential first step toward protecting your sensitive conversations, but it's important to remember that security is about more than just the tools you use, it requires **consistent practices and vigilance**. Simply relying on a secure app for certain discussions while **using less secure platforms for related conversations can expose vulnerabilities**. Doing so can compromise the very security you're aiming to protect, as attackers can piece together information from different sources to build a bigger picture.

Ensure that all your devices, whether it's your smartphone, tablet, or computer, **are regularly updated with the latest software patches and security updates.** Outdated software can have vulnerabilities that attackers exploit.

Avoid sharing your devices with others. Even if you trust those around you, **sharing your device opens up the possibility for unintentional security lapses.** For instance, someone could **unknowingly download malware, change security settings, or access sensitive information.**



Activate disappearing or auto-delete messages. These options automatically remove conversations after a set time, **reducing the risk of sensitive information being stored or retrieved if your device falls into the wrong hands.** This not only **minimizes your digital footprint but also limits the amount of data that could be exposed in the event of a security breach, device confiscation or device loss.**



Maharat Foundation

Address:
Jdeideh, Metn
Beirut, Lebanon

Contact Information:
Website: maharatfoundation.org
Email: info@maharatfoundation.org

مهارات
Maharat