Messenger

> [!toc] Table of Contents

While emails are still regularly used for digital communication, messengers have become more popular in recent years.

One advantage of (good) messengers over emails is that encryption and secure communication are part of their initial design, while email is unencrypted and rather insecure by default.

Some criteria for what constitutes a good messenger can be found at PrivacyGuides. For activists, depending on the threat model, it is particularly important to have secure and anonymous communication.

Two messengers that are widely used in activist circles and can be recommended are Signal, Matrix and Delta Chat.

> [!example] TL;DR {static}
>
> **Signal** sets the highest standards for it's encryption and data protection and is probably the easiest to use. The disadvantage: it requires a phone number for registration.
>
> **Matrix** also uses modern encryption, but can be less intuitive to use. It is decentralized, meaning you can choose a server you like for registration and don't need a phone number.
>
> **Delta Chat** relies on old email protocols uses PGP for encryption. PGP is still considered secure. However, if your private key is stolen by an attacker, the whole communication history can be leaked. The advantage of Delta Chat is it's decentralized and that you just need a working email account to get started.

Signal

Signal was developed by the anarchist Moxie Marlinspike and is one of the best-known alternatives to the monopolist messenger WhatsApp.

Advantages of Signal

- **Easy to use**: Signal is simple to install and everything “just works.” There isn't much you can do wrong that would compromise security.
- **Widespread use**: As of January 2025, the platform had approximately 70 million monthly active users. While this is still far behind WhatsApp's 2 billion users, it is nevertheless widespread, in contrast to some other Messengers in this list.
- **Secure encryption**: Signal has its own communication protocol that is open source and regularly audited. Some other messengers, such as WhatsApp, have also adopted the protocol, meaning that it is used daily by billions of users. Communication in Signal is therefore securely end-to-end encrypted.
- **Data minimization**: Signal stores as little as possible about its users and can therefore only disclose very little information when forced by authorities to hand over user data. The only data that Signal *was able to* disclose in past court cases was the date the account was created and the date the account was last used. When legally forced to provide information to government or law enforcement agencies, Signal discloses the transcripts of that communication here.
- **Option for automatic deletion**: Chats can be set to automatically delete messages after a certain period of time. This means that they are secure even if the police gains access to the device (but only after this period).

Disadvantages of Signal

- **Anonymity**: Signal was not designed to be anonymous, but to provide secure encryption. As of today (December 2025), a phone number is required to register. In many countries, phone numbers must (legally) be registered to a real person. The phone number used to be visible to everyone you communicate with, but Signal now enables users to hide their phone number from other users. When using a phone number that is not linked to your identity for registration, Signal can therefore be considered as anonymous as the other messengers in this list.
- **Based in the US**: The Signal Foundation is based in the US and can therefore be forced to to hand over data to intelligence agencies. However, Signal has very little data that can be handed over.
- **Centrality**: Signal only runs on its own infrastructure (which is located at Amazon, Microsoft, Google, and Cloudflare) and cannot be self-hosted. This means that users must

trust Signal to some extent to do its job well. On the other hand, a compromised signal server does not mean that all your chats are also compromised, as long as your security numbers stay verified. But, it does mean that there is a central point of failure: If signal gets shut down one day, you may need another channel of communication to your contacts.

- **Censorship**: Since Signal is centralized, it is possible for governments to try to block connections to Signal servers. While Signal introduced proxies that can bypass censorship, it makes the bar-of-entry higher. Statistics from other projects such as the Tor project show that usage of a technology significantly declines when it is censored, even if there are ways to circumvent it. The plans of the EU to possibly introduce "Chat Control" and Signal's response that they may will exit the European market if the proposed regulation is passed highlight this issue. If the law passes, EU users may need to rely on proxies to connect to Signal or fallback on alternative messengers

Signal groups

Signal groups are popular and frequently used for communication in larger groups *(up to ~150 contacts)*. In general, Signal chats offer automatic deletion of messages after a set period of time, which should also be set for groups that have a higher risk potential.

Unfortunately, there is no function yet that automatically deletes entire groups after a set period of time. Therefore, especially when devices are confiscated, it is important to consider which contacts are connected in which groups *(or which group names!)* and could also be compromised.

We therefore recommend *(for all group chats, not just on Signal)*: Based on the principle of *plausible deniability*, give your groups names that are as inconspicuous as possible and that cannot be used against you! In case of doubt, the chat history will only show **that** the group name has been changed, but not what the group was called before.

> [!danger] Attention {static}
>
> In the event of confiscation, the affected account should also be removed from all groups immediately!

> [!tip] {static}
>
> You can read our instructions on how to use Signal as anonymously and securely as possible.

Matrix

Matrix is a communication protocol. There are various client apps for this protocol, the best known being Element.

Matrix has become increasingly popular in activist and hacker circles, especially in recent times.

How it works

The most important difference between Matrix and other messengers, such as Signal, is its decentralization, or *federation*. Similar to email, there are many different servers (*"home servers"*) (such as *matrix.org* or *matrix.systemli.org*). If an activist with a Matrix account at matrix.org communicates with an activist with a Matrix account at matrix.systemli.org, the (encrypted) messages must be synchronized between the two servers.

Matrix Federation Functionality

Advantages of Matrix

- **Secure encryption**: Matrix uses its own implementation of the Signal protocol. It has some disadvantages compared to the Signal protocol, but is still similarly secure.
- **Decentralization**: Matrix is federated and therefore decentralized. There are many different servers that communicate with each other, so there are many points that would have to be attacked to completely paralyze Matrix. It is therefore more resistant to censorship then Signal, both legally and technically.
- **Anonymity**: Some servers do not require any personal information to create an account. This makes it possible, in principle, to use Matrix anonymously.
- **Openness**: The source code of Matrix and Element is open source and can be audited for security.

Disadvantages of Matrix

- **Complicated to use**: Matrix can be complicated to use at times. The principle of federation is counterintuitive for non-technical people, there are many different clients to choose from (which be overwhelming), and some things do not work smoothly yet.
- **Not yet widely used**: People often need to be persuaded to set up a Matrix account.
- **Lack of data minimization**: Because Matrix is federated, all data must be synchronized across all federated servers. This also means that it is practically impossible to delete

data. By default, the Matrix ID, personal information, usage data, IP addresses, device information, other servers with which communication takes place, and room IDs 1 are stored on all servers by default.

> [!info] {static}
>
> Overall, choosing the right messenger depends on the threats you face, the people you want to communicate with and personal preference. From a technical and security perspective, the above, especially Signal, are most recommended.

[1]: The source refers to an older version of Matrix. It is unclear to what extent the amount of data stored by default and the deletion behavior are transferable to current versions.

Version #2
Erstellt: 2026-02-15 16:16:34 UTC von ESC-IT Migration Bot
Zuletzt aktualisiert: 2026-03-18 13:28:22 UTC von ESC-IT Migration Bot