Messaging Apps: Choosing an App

An overview of messaging apps and detail on the four main ones: WhatsApp, Telegram, Mattermost and Signal

Messaging Apps Overview

As a decentralised network, there is no one communication tool that everybody uses. That can sometimes make it tricky to connect with people. Don't worry, you're not alone!

To help you create a group chat, we will compare four apps most commonly used by XR groups.

Ultimately the app you choose comes down to what you and the other people are comfortable with, including how safe and secure you need to be. If security and organisation are your priority, you may well choose more than one app and use them in combination.

To help minimise information overwhelm, try to plan what chats you need carefully and use existing chats where possible, rather than creating more new ones.

> Communication channels for a specific actions work a bit differently. If you need secrecy and safety, create temporary channels with just those who need to know (with disappearing messages) and use "airgapping" to break up the information flow where appropriate. Delete these channels after use. Head over to this page for lots more detail on how to do secure internal comms for an action.

Our recommendations can be summarised as:

If your group...

- **...organises lots of different things at once**, use Mattermost. The extra features and discoverability should really help to make your group more productive.
- **...organises a lot of actions**, use Mattermost combined with Signal for the added security.

Overview

WhatsApp

WhatsApp is widely used by people outside of XR but it is not secure so is not great for organising. It doesn’t sync up with Mattermost.

However, Whatsapp Communities can be very useful for keeping all of your (non-spicy) comms in one place. A community is a collection of chat channels, and individuals can choose which ones to

join. Each community also has a central Broadcast-only channel.

More detail on WhatsApp here.

Telegram

Telegram is used for XRUK's broadcast channels.

It’s an encrypted messaging service with lots of features. You can edit and pin messages, see the chat history after you join a channel, locate media, and each chat can hold a large number of people. It’s also accessible on nearly any device. A limit on message word count can impact broadcast posts.

Telegram has some good features that Whatsapp does not have.

However, there have been recent concerns about the security of Telegram, as not all messages are End to End Encrypted and there is a lack of transparency around who Telegram is sharing its data with.

More detail on Telegram here.

Mattermost

We run our own dedicated communication tool, called Mattermost (if you're famililar with Slack or Microsoft Teams, it's a bit like those). We host it on our own secure servers powered by renewable energy and it is accessible on both phone or computer.

It is used by most XRUK teams and is also available to all groups. It's a great way to connect to any group or team in the movement: look for the dozens of "reception" channels, where you can pop in to ask questions. You can also connect directly with individual users by direct message.

However, users who are not used to this sort of platform can sometimes find it overwhelming or confusing, which is why many local groups choose other platforms.

There is lots of help and support here on Rebel Toolkit.

More detail on Mattermost here.

Signal

Signal is widely used by action planning groups and organisers. It’s the most secure encrypted chat with a disappearing message function. It’s also visually clean and crisp.

However, it’s not possible to pin or thread messages or edit your messages after 15 minutes, making it less useful for mass communications.

More detail on Signal here

Summary Table

	WhatsApp	Telegram	Mattermost	Signal
Security	★★	★★	★★★★	★★★★★
Accessibility	★★★	★★★	★★★★	★★
Features	★★★	★★★	★★★★★	★★★
Discoverability	★★	★★★	★★★★★	★★

Security and Discoverability

Why does security matter?

Given the types of actions XR does, **it is essential that the authorities do not get access to rebels' personal information and private messages**. This is for a number of reasons including:

- It could compromise the legal defences of arrestees
- It could affect the right of rebels to stay in the UK

When discussing security in the context of messaging apps, there are two main things to think about:

- Can my messages get intercepted?
- Where are the messages getting stored?

The first of these is straightforward - to make sure messages cannot be intercepted we need to make sure that the app uses secure encryption when sending messages. The second, however, is a little more complicated as it depends on terms like "end-to-end encryption".

End-to-end encryption is used by a number of messaging apps. What it means is that the messages are stored on the phones sending and receiving the messages, rather than on some server. This is generally good from a security standpoint because the authorities would need to access one of the phones in order to see the messages; something much harder for them to do than approach the owners of the server with a warrant.

Another important things to consider when choosing a messaging app is whether or not you want to have disappearing messages. These are messages that are automatically deleted after a certain time period, usually around a week or so. This can provide an additional layer of security on top of end-to-end encryption.

Lastly, one extremely important thing to bear in mind when discussing security is that **by far the biggest weakness in XR's security is the people**. It is very easy for an undercover police officer to pose as a protester and get themselves added to a 'secure' group chat. Once that happens, any security features of the messaging app become irrelevant since the authorities can see everything that is getting discussed.

If you're organising actions, head over to the Internal comms for your action page to read about chat security in more detail.

Why does discoverability matter?

Discoverability - making your group easy to find and get in touch with - is a huge issue for XR. We are a decentralised organisation so each group has the freedom to decide how they want to organise and communicate. This is fantastic from the point of view of self organising, but it makes it difficult to share knowledge and skills across groups. To try and reduce this problem, it is important when choosing a messaging app to think about how other rebels and groups can find your group and get in touch with you.

WhatsApp

WhatsApp is a hugely popular messaging app with over 2 billion uers. It's easy to use and the vast majority of rebels will already have it installed on their phones. Does this make it a good fit for your XR group?

Security

Despite being end-to-end encrypted, WhatsApp has a number of serious security issues that make it a poor choice for serious organisation in XR. To start with, it is owned by Facebook, a company whose income depends on collecting people's personal information. They can't read your actual messages, but there's still lots of metadata they can collect. You can read WhatsApp's privacy policy to get an idea of the sorts of information that they are collecting.

Another issue with WhatsApp is that it makes it easy to backup chats to a cloud storage like iCloud or Google Drive, and that the option to make these backups encrypted is off by default. That means that any user in your chat who has a backup running (which is common) and hasn't manually set this to be encrypted will be uploading the whole chat (their messages and everybody else's messages in the shared chat) to a server. The data on that server can be read by the company or by security services with a warrant. However, you can now add End to End Encryption to this backup.

Accessibility

WhatsApp has a lot in common with other messaging apps so it is usually quite straightforward for rebels to learn how to use it. However, in order to sign up to WhatsApp you need a smartphone, which not all rebels will have access to. In order to use WhatsApp on a computer, the smartphone that it's linked to must be connected to the internet continuously, which is a hindrance.

Features

You can't save messages for later or mark them as unread so you constantly lose key info and can't find it again. However, you can pin key chats so that they remain at the top of the chat list. The message box is small and you can't thread effectively so it is difficult to keep track of a conversation.

Whatsapp have recently launched a new feature called Communities, which allows you to collect together multiple chats for your group into one space. Each community has a broadcast only channel that everyone in the community is subscribed to, and then you can add as many sub-groups as you like. This means chats can be arranged by topic, making it easier to keep on top of conversations. Each member can choose which chats they want to join, reducing information overwhelm from being in too many chats.

Discoverability

Within WhatsApp, group admins can create and share links that rebels can follow to sign up to the group. This provides a quick and easy way to invite new people. However, unless this link is published somewhere for rebels to find, it is impossible to find the group to join in the conversation.

The Whatsapp communities feature improves discoverability of channels once a person is in that community, as all chats connected to one group can be connected together.

Other information

Another issue with WhatsApp is that many people use it to speak to friends and family. Having XR-related chats on the same platform can put unnecessary stress on rebels who might want to temporarily 'switch off' XR communications in order to avoid burnout.

Telegram

Telegram is a great messaging app filled with features. In particular it has broadcast channels which can be fantastic for sharing information widely. But is it suitable for group chats?

Security

Although Telegram's website would have you believe otherwise, Telegram actually provides the worst security out of all the apps being compared here [1] [2].

One of the reasons why this is the case is because **Telegram group chats are not end-to-end encrypted**. Telegram does allow users to have secret chats with self-destructing messages. However, this is not available for group chats so all of the messages that you send to a group chat will be stored on a server somewhere accessible to the authorities.

Another serious problem with Telegram's security is that **messages are sent using Telegram's own private encryption protocol** as opposed to something used more widely. This means that it has not been as thoroughly tested and many security vulnerabilities have been exposed in the past.

It can be compromised if malware is installed on the phone or computer, or other people have access to that device if they use your login. Or if you have infiltrators - no app protects against those.

Accessibility

Telegram is one of the most accessible apps available. You don't need a smartphone to sign up, just a phone number, and it can be used on practically any device.

Features

Telegram is very useful for broadcast channels in which only admins can post. Links for these can then be shared on wider channels, e.g. Rebellion Broadcast. However, widely shared links attract spammers so they need to be carefully moderated.

Discoverability

Telegram has some excellent features that make group chats easy to find and join. Like Signal and WhatsApp, users can share a link to the chat that people can use to join it. However, you can also search for public Telegram channels from inside Telegram. This makes it easy to find and contact broadcast groups but can also lead to spam since anyone can join these channels - even if they are not a member of XR.

Use this information to help you hide your details from spammers.

And this information about removing spamers.

Drawbacks

Telegram is really a social media platform and has a very ‘relaxed’ content moderation strategy- this means it is targeted by spammers if you have open channels. You have to be on top of moderating it!

Some people find it difficult as you can't save messages for later or mark them as unread so you constantly lose key info and can't find it again. However, you can pin key threads at the top of the chat list.

It's limited in terms of formatting messages and if you want to broadcast and add an image there's a character limit so you have to be able to either fit your message into that limit or miss out key info.

Mattermost

Mattermost is the messaging app that has been specially set up by XR for rebels to collaborate with each other. It is quite different to the other apps being discussed because it is designed to be used by teams in a workplace as well as for personal communications. Unlike the other tools, it also exclusively runs off of renewable energy.

Security

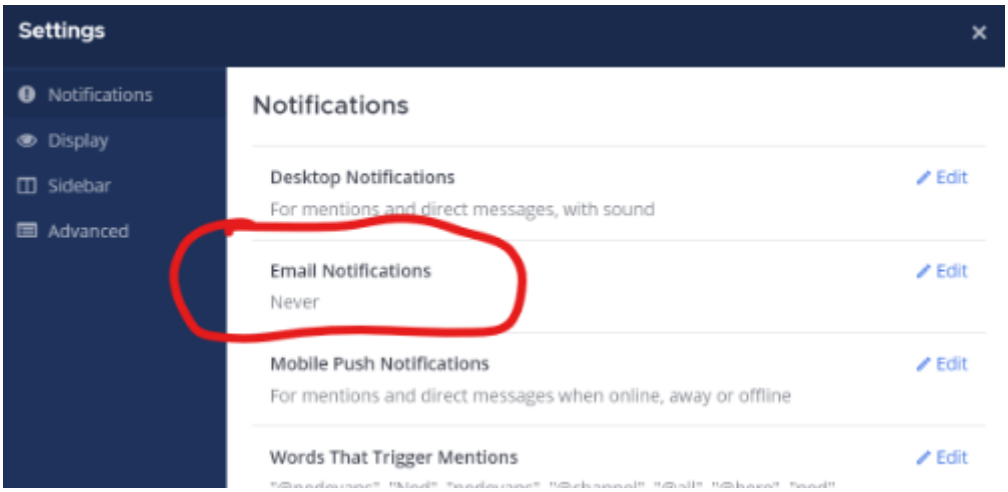
Mattermost takes quite a different approach to security than the other apps. Instead of employing tactics such as end-to-end encryption and self-deleting messages, Mattermost prevents the authorities from accessing your group's messages by storing them on our own secure server.

Its great to use Mattermost as one of your channels if you are **air-gapping** to separate out information on a need to know basis.

Another great advantage to using Mattermost is that if rebels ever get arrested, they can have their accounts temporarily suspended so the police would not be able to read any messages even if they took a rebel's phone. Once the rebel gets out of custody they can then have their account reactivated.

Can be compromised if malware is installed on the phone or computer, or other people have access to that device if they use your login. Or if you have infiltrators - no app protects against those.

PLEASE NOTE: If you are discussing anything 'spicy' / illegal, ensure all members of your private Mattermost channel or group Direct Message, have their email notifications set to **Never**. This adds a level of security as emails potentially can be compromised or 'hacked'. To check your notifications, select the Settings icon - Notifications - Email Notifications - Edit - Never - Save.



Accessibility

You do not need a smartphone to sign up - only an email address - and you can easily use it on any device unlike some other apps (e.g. WhatsApp) that only work if linked to your phone.

If you have a computer it is very easy to use since you don't have to install anything - just use your browser. This also means that the messages can be easily read on a larger screen.

However, some rebels who are less 'techy' find the different format of Mattermost (as opposed to a messaging app like Whatsapp or Signal) very confusing, which is why Mattermost isn't used by some Local Groups.

Features 

Mattermost has by far the most features out of the apps being compared. It is specifically designed for use by teams, as opposed to personal messaging, and so has a number of advantages over the other messaging apps.

For example, in Mattermost chats are organised into teams, public channels, private channels, and direct messages. This makes it easy to navigate between different chats. Also, Mattermost has a much better way to handle multiple conversations happening in the same channel at once. Whilst the other apps allow you to quote reply to individual messages, Mattermost has threaded conversations so you can see the full history.

You are also able to **save messages** for yourself which makes finding links and key info much easier, **mark messages as unread** to revisit later, **pin** important messages so other people in the chat can find them easily and **store regularly used links such as minutes and meeting links in the Channel Header** for everyone to use, removing the need to bookmark/store those links on

personal devices.

Writing messages in Mattermost is also more powerful. Not only are you able to edit your messages after you've sent them, but you can use Markdown to format your messages in fancy ways. Great for making eye-catching announcements!

There is a small learning curve when you use Mattermost for the first time because, being designed for teams, it is laid out differently to the other apps. The design is practically identical to other popular messaging apps like Slack and Discord so if you are familiar with those you will have no issues.

Discoverability

One of the main reasons why XR uses Mattermost is to make groups discoverable. Every group that signs up to the XR UK Hub will have public and private group chats created on Mattermost for them as the Hub does the 'heavy-lifting' for you. Having your group on the Hub means the Hub does the work of creating your Mattermost channels (as well as Cloud folder and Forum spaces) and the group's members will be joined automatically to the group's chats and at the same time, given access to the Cloud folder and Forums.

Every group that signs up to the Hub gets a public group chat called a **Reception** channel so, if you're not a member of the group, contacting the group is as simple as searching for and joining the group's Reception. Having publicly discoverable Receptions is a major advantage over other apps as you can quickly see if a channel already exists for a specific group or topic. After joining a Reception you can then chat to the group and if you want to get more involved, you can be sent a Hub invite to the group which automatically adds you to the group's private channel. You can't search for chats on WhatsApp and Signal and can only find big public channels on Telegram which leads to similar channels being regularly created for the same purposes on these other apps. This can lead to burn-out for chat Admins as well as rebels when they need to monitor multiple chats for the same group/action.

You can also use the Hub Groups List to find other groups and get information such as their email address, website and social media account.

This is why **we strongly recommend that your group at least signs up to Mattermost and the Hub** as it provides an easy way for other groups to get in touch with you.

Signal

Security

Signal has the best security out of all of the apps compared here. Chats are always end-to-end encrypted and you can enable disappearing messages.

Furthermore, Signal is actually open-source. This means that anybody can look at Signal's source code and verify that it is secure.

Signal has been designed with security in mind, not bolted on afterwards, so the defaults are more likely to be good.

Signal PIN is a useful application lock, although this isn't set up on the computer version.

Signal encrypts local information on your computer or phone so that it's only visible through the app or computer programme.

It can be compromised if malware is installed on the phone or computer, or other people have access to that device if they use your login. Or if you have infiltrators - no app protects against those.

Accessibility

People aren’t normally familiar with Signal before joining XR so may be a barrier to newcomers or less technical users.

Has complicated features like Signal PIN which can be a barrier to use.

It is available on computers, although it'll still be tied to your phone number.

Features

Signal has many of the same features as WhatsApp and Telegram. Whilst this makes it easy to learn how to use, it also means that:

- It is hard to write longer messages in the small message box
- It is difficult to keep track of multiple conversations happening at once
- Once you have sent a message it can't be edited
- Can be used on smartphone and computer versions

Discoverability

Just like WhatsApp, you can share links to Signal group chats allowing people to quickly join the group. This is great for signing people up, but it is hard for rebels to find this link and join the group.

Drawbacks

It can be hard to know who is on a Signal chat, as names can be changed and phone numbers hidden. Like with all chat apps, be careful who you are talking to if that's important.

Signal can also be problematic for rebels who have limited storage on their phones because the messages are stored locally instead of in the cloud, and this can take up a lot of space.

The "metadata" about who's using the app and where they appear to be may be available to the authorities if they can track the connections to the central computer server, or get access to that server.