Choosing a messaging app for your XR group

If you want to create a group chat for your XR group, there are loads of different options and making the right choice can be difficult. In this document we will compare the four apps most commonly used by XR groups: WhatsApp, Telegram, Mattermost, and Signal - which should help you to decide which is best for your group.

We have broken down the comparison into four categories:

- **Security** - How easy is it for the authorities to access your personal information and read your messages? (see the Appendix for more information)
- **Accessibility** - How easy it is for rebels to use the app?
- **Features** - What features does the app have that allow you to organise effectively?
- **Discoverability** - How easy is it for rebels to find and join the group? (see the Appendix for more information)
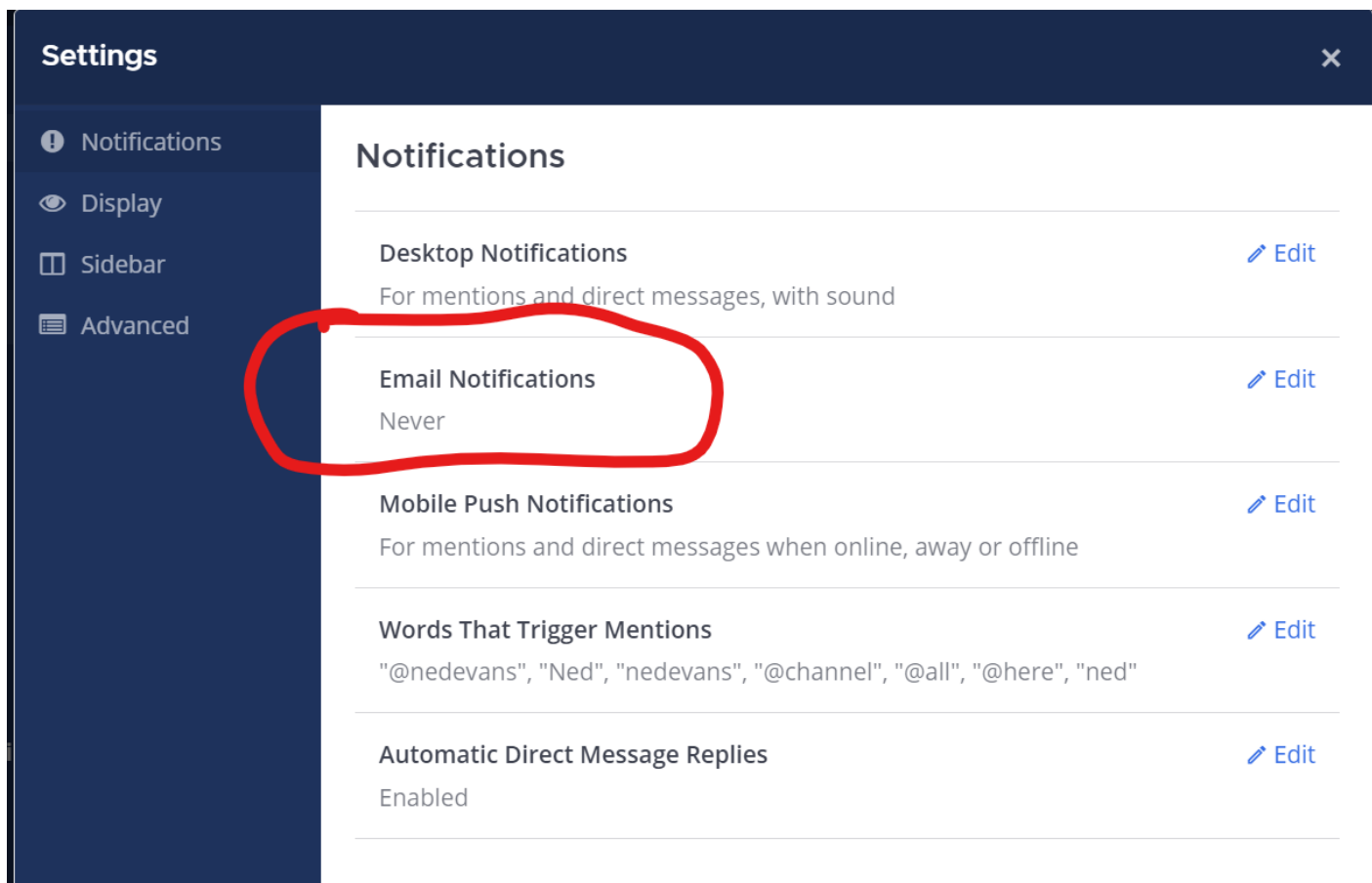
Key Security Information

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.

The best thing to do to protect ourselves and XR is to use a process called **'Air-gapping'** and is broadly used in government agencies, military and corporate sectors. It's a trick they don't want us activists to know and use!

Air-gapping simply means we communicate any action planning and organising using a **private** Mattermost channel or direct message and then send specific details such as car registrations, credit card numbers and addresses using an app that is end-to-end encrypted and has self-deleting messages (Signal is best). This creates a gap between the planning and those specific details and ensures that if an adversary manages to get their hands on one account, they don't have all the pieces of the puzzle to sabotage an action, nor pair up individuals with a particular action plan, nor put faces to words with intent to commit crime (etc).

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.

Settings

Notifications
Display
Sidebar
Advanced

Notifications

Desktop Notifications   ✎ Edit
For mentions and direct messages, with sound

Email Notifications   ✎ Edit
Never

Mobile Push Notifications   ✎ Edit
For mentions and direct messages when online, away or offline

Words That Trigger Mentions   ✎ Edit
"@nedevans", "Ned", "nedevans", "@channel", "@all", "@here", "ned"

Automatic Direct Message Replies   ✎ Edit
Enabled

Summary

If you don't want to read the comparison page in full, here is a quick breakdown of the different scores for each messaging app:

	Whats-App	Telegram	Matter-most	Signal
Security	★★	★★	★★★★	★★★★★
Accessibility	★★★	★★★	★★★★★	★★
Features	★★★	★★★	★★★★★	★★★
Discoverability	★★	★★★	★★★★★	★★

Ultimately which tool you decide to go with comes down to what you and the other people in your group are comfortable with. However, 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. Also don't forget to enable disappearing messages.

WhatsApp

WhatsApp is a hugely popular messaging app with over 2 billion users. 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. You can read WhatsApp's

[privacy policy](#) to get an idea of the sorts of information that they are collecting.

Another serious and often overlooked security issue with WhatsApp is that its end-to-end encryption often does not work. Most WhatsApp users enable an option called 'Chat Backup' so they can recover their messages in case they lose their phone. If this option is enabled, for even a single person in a WhatsApp group, then that means that all of the group's messages will be stored, unencrypted, on either a Google or Apple-owned server, freely accessible to the authorities.

Verdict: ⭐⭐

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.

Verdict: ⭐⭐⭐

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. The message box is small and you can't thread effectively so it is difficult to keep track of a conversation.

Verdict: ⭐⭐⭐

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.

Verdict:

⭐ ⭐

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 (source, source).

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.

Verdict: ⭐ ⭐

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.

Verdict: ⭐ ⭐ ⭐ ⭐ ⭐

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. The message box is small and you can't thread effectively so it is difficult to keep track of a conversation. 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.

Verdict: ⭐ ⭐ ⭐

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.

Verdict: ★ ★ ★

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.

The best thing to do to protect ourselves and XR is to use a process called **'Air-gapping** and is broadly used in gov agencies, military and corporate sectors. It's a trick they don't want us activists to know and use! Air-gapping simply means we communicate any action planning and organising using a **private** Mattermost channel and then send specific details such as car registrations, credit card numbers and addresses using an app that is end-to-end encrypted and has self-deleting messages (Signal is best). This creates a gap between the planning and those specific details and ensures that if an adversary manages to get their hands on one account, they don't have all the pieces of the puzzle to sabotage an action, nor pair up individuals with a particular action plan, nor put faces to words with intent to commit crime (etc).

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.

Verdict: ⭐⭐⭐⭐

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.

Verdict: ⭐⭐⭐⭐⭐

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 eeting 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.
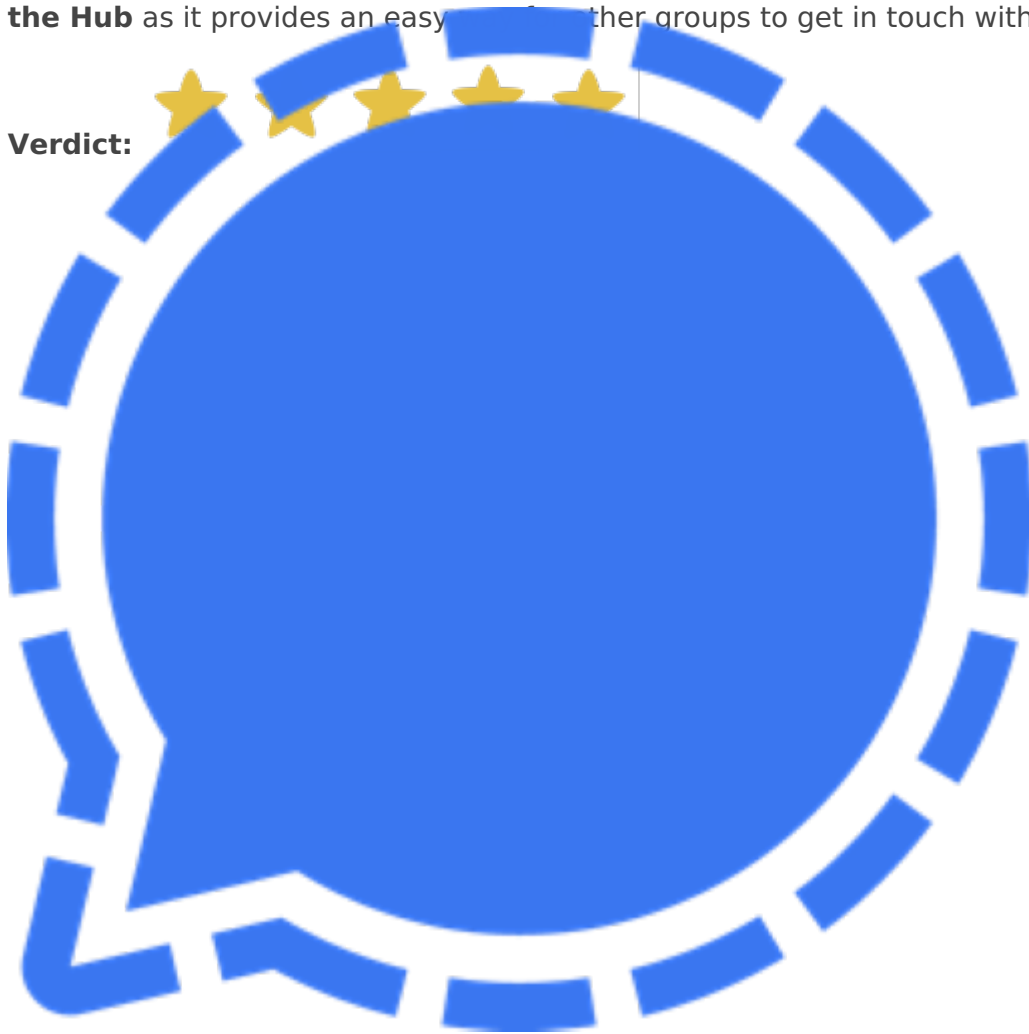
Verdict: ⭐⭐⭐⭐⭐

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 public 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 there often isn't the capacity to administer these additional chats and in addition, rebels get added to multiple chats for the same group increasing the number of chats they need to monitor which quickly leads to individual burn-out.

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.

Verdict:

Signal

Security

Signal has unquestionably 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.

Verdict: ★ ★ ★ ★ ★

Accessibility

Has complicated features like Signal PIN.

Verdict: ★ ★ ★

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

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.

Verdict: ★ ★

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.

Verdict: ⭐ ⭐

Appendix

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.

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 mitigating for power, 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 the group and get in touch with you.

Alternative messaging apps

There are many other messaging apps used by rebels in XR. We have just chosen to focus on the most commonly used ones here. Some other popular choices include:

- Discord: An app with some great features but extremely poor security and privacy.

Useful links

- Electronic Frontier Foundation: Thinking About What You Need In A Secure Messenger
- A Guide to Group Chats on Signal, Whatsapp and Telegram book on the Rebel Toolkit