

Comparing Security of Signal, Telegram and WhatsApp

Signal

- Signal is by far the most secure encrypted channel option.
- When you use Signal, your data is stored in encrypted form on your devices.
- Signal also has disappearing messages (self-destructing messages) which the other channels do not, which are an essential security feature
- Signal is free and all you need is a smartphone.
- Unlike Telegram, which also benefits from end-to-end encryption in its “secret chats”, Signal has the feature enabled by default so you won’t have to take any additional steps to get this, and that is why it is used for actions over and above everything else.

Telegram

- End-to-end encryption is not automatically used on messages sent in Telegram.
- Telegram is really a social media platform and has a very ‘relaxed’ content moderation strategy- this means it is targeted by spammers. You have to be on top of moderating it!
- Telegram is very useful for broadcast channels (in which only admins can post). Links for these can then be shared on wider channels (eg. Rebellion Broadcast). However, widely shared links attract spammers so they need to be carefully moderated.

WhatsApp

- End-to-end encrypted but owned by Facebook therefore its privacy is not reliable. WhatsApp also collects more metadata on you than apps like Signal.
- We do not recommend that anyone uses WhatsApp for actions, even those that are ‘non-spicy’ just in case.

- Some groups choose to use WhatsApp as more people already have it downloaded, but due to the security issues described above we strongly recommend groups use Signal for all of their organising.

See Also

[Choosing a messaging app for your XR group](#) in the "Online Tools for Communicating with Other Rebels" book.
