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.
