



National Cyber Security Centre
Ministry of Security and Justice

Choosing a messaging app for your organisation

Publicly available apps are being used for business communication

Factsheet FS-2017-03 | version 1.2.1 | revised November 2022

A large part of business communication is conducted through messaging apps.¹ Using publicly available messaging apps for business communication involves certain risks and has consequences for both your organisation and information sharing. Of the messaging apps currently in use, few are sufficiently secure to comply with your security policy for internal communication.

The NCSC recommends that you assess which messaging app is most suitable for use within your organisation. You should then conduct a risk analysis which takes into account your organisation's security and user requirements and take further action if required.

Background

Using messaging apps to share confidential business information involves certain risks. This factsheet describes the main risk factors involved in the use of messaging apps. Its objective is to provide information security officers with the information they need to conduct a risk assessment to find a messaging app that is most suitable for use within their organisation. The NCSC recommends that organisations conduct a thorough research before choosing a messaging app, to ensure it complies with their internal security policy. The NCSC itself does not assess the security of messaging apps.

Target audience

Information security officers at medium-sized and large organisations.

The following organisations have contributed to this factsheet:

The Tax and Customs Administration, the Nuclear Research & Consultancy Group (NRG) and Rabobank.

¹A messaging app is an online communication service for smartphones. Examples include WhatsApp, Signal and Telegram. Such apps are used to exchange information. This factsheet does not cover instant messaging

(IM) services, such as Slack and the Extensible Messaging and Presence Protocol (XMPP).

What is the matter?

Messaging apps are often the platform to communicate quickly with each other.

Messaging apps are often used as a means of communication. This is due in part to the user-friendliness and ready availability of these apps. Their ease of use enables more efficient cooperation and communication with colleagues and clients. Many messaging apps are supported by multiple operating systems. They can usually be run on smartphones and occasionally also on laptops. In many cases, messaging apps are free and easy to install. Moreover, the chosen app will usually be familiar to many colleagues and clients, as they already use it privately. The opportunities offered by such apps present a sharp contrast with the often limited functionality offered by the organisation.

There are risks attached to the use of messaging apps.

Using messaging apps involves a number of risks, the main one being that data may be received by other parties than the intended recipient. In other words, the wrong party may receive confidential information by mistake. This may constitute a data breach. In addition, the telephone number you used may no longer be in use by the intended recipient.

When using messaging apps, organisations and their employees do not always consider the risks involved.

Using messaging apps for business communication involves certain risks. It is the responsibility of the organisation to ensure that the employees are aware of the need to use a messaging app which complies with its internal security policy as much as possible. The risks to which the organisation is exposed pertain to the location of the data, who has access to it and which parties are able to request it. The linking of databases following a merger or takeover is but one example of how data may end up in the hands of other parties or at another location. If data are stored outside of the country, a different jurisdiction may apply.

What could happen?

Your organisation needs to conduct an assessment to determine the level of its exposure to the risks mentioned above. Other factors to be considered in such a risk assessment include the maturity of your organisation and the potential impact of the risk. If your organisation has Mobile Device Management (MDM) in place, some risks may not apply or only to a limited extent. MDM allows an organisation to place an app inside a container and manage it autonomously. Determine the level of exposure of your organisation to each of the risks below.

Entire contact lists are uploaded to the servers of an app developer.

During the messaging app's installation, a pop-up may appear requesting access to the phone book. This may be useful in some cases, as it allows the app to import all contacts straight away and the user to launch a chat easily. However, it involves

uploading the phone numbers of all the contacts in the phone's memory to the servers of the app developer. In other words, the phone numbers in the smartphone are copied to another location. The question is to what extent this constitutes a risk for your organisation. It may be the case that the phone book lists persons in a sensitive position or with a secret number. The third party will also have come into the possession of the phone numbers of colleagues or clients, who won't be aware that the third party possesses their data. Consider the legal ramifications for your organisation, e.g. with regard to its privacy policy and any contracts or non-disclosure agreements signed with business partners. Such agreements may contain clauses preventing the sharing of client data with third parties.

Behavioural and user data are stored elsewhere and can be requested by third parties.

Messages sent by messaging apps are usually accompanied by behavioural and user data, which are transmitted in the background. By analysing these data, other parties may be able to infer who was in contact with whom, at what time and how often. These data may also include user statuses and profile pictures.² In addition, such data may be stored on servers in foreign countries, in which case different laws and regulations apply. This potentially allows third parties to access and share the data without permission. Foreign intelligence agencies may request such data if they are stored on servers which fall under their jurisdiction.

Other parties are able to view the contents of messages.

If network traffic is not sufficiently encrypted, external parties will be able to intercept it and view the contents of messages. Both foreign intelligence agencies and criminal organisations are keen to intercept network traffic, and have the means to do so.

Confidential information ends up on servers outside of the organisation's network.

Data may be transmitted to an external server even before the messaging app is fully installed. Whether and for how long messages are stored on the server depends on the individual messaging app.

The server may be located anywhere in the world. Your organisation neither manages the server nor has an overview of the data that have been transmitted to it. By consequence, your organisation is reliant on the security of a third party with which you have not entered into an agreement.

Legal and organisational risks

Your organisation must treat data, including personal data, as confidential and implement suitable organisational and technical data protection measures. Any loss of confidential information by your organisation may lead to reputational damage. Financial damage may be incurred if you are fined or if people lose trust in your organisation or its products. In some cases, fines may be imposed for data breaches. Take note

² See also <https://veiliginternetten.nl/thema/draadloos-internet/berichtendiensten/mijn-locatie-zichtbaar-whatsapp>

of the legal requirements that apply to your sector in order to comply with its obligations. In example for the disclosure of written communication and logging of the necessary communication that contributes to the internal and external quality checks, audits and the requirements of the supervisory authority.

What does the NCSC recommend?

Conduct a risk assessment to determine whether the use of a messaging app within your organisation is desirable and appropriate.

Each organisation is different. Logically, this difference extends to the level of risk organisations consider acceptable. Whereas some organisations impose no protection framework and allow the use of all messaging apps, others aim to find the safest messaging app to use. Yet other organisations develop and manage their own messaging apps for internal dissemination. The extent to which the risks outlined above are applicable and acceptable depends on the organisation's level of maturity and on its MDM policy, which varies from organisation to organisation. The risks outlined above provide criteria for an assessment of messaging apps and a comparison of the outcomes to your organisation's existing security policy. Share the outcomes with business partners, taking into account the high rate of obsolescence of some messaging apps and the functionality they offer. A joint assessment of messaging apps will provide an insight into the risks involved. A thorough assessment will reveal which messaging app is the most suitable one for your organisation or whether developing and managing your own internal messaging app is the only viable alternative. Choose the messaging app that comes closest to complying with the security requirements of your organisation's security policy for internal communication and other internal guidelines.

Check whether your internal security policy covers the use of messaging apps.

Check whether the use of messaging apps is covered sufficiently in your internal security policy. Evaluate your existing policy and examine closely whether it applies to the use of messaging apps for internal communication. If the risks involved in the use of messaging apps within your organisation are not adequately addressed by your existing policy, you should add specific requirements.

Determine which messaging apps comply with your security policy to provide an acceptable level of residual risk.

The selection and use of a messaging app is dictated by your internal security policy. Assess the usage terms and conditions, security measures and functionality of each messaging app. Determine whether these factors are sufficiently compliant with your internal policy. If not, compile a list of discrepancies and take further action. Choose the messaging app that comes closest to meeting your current security standards, thereby limiting the level of residual risk and the need for further measures.

Take further action if required.

Once you have checked and assessed your security policy and examined potential messaging apps, you will need to evaluate your existing set of security measures. Your current technical and organisational measures should be sufficient to cover the risks. If not, take remedial action in order to manage residual risk. Your organisation's MDM policy is also relevant in this respect.

Additional security measures for messaging apps include:

- installing messaging apps from a recognised app store only;
- choosing a messaging app which does not upload contact details/your phone book to a server;
- creating an internal or secured address book/contact list for your organisation for use with the app;
- choosing an app which offers the possibility to authenticate the communication channel (e.g. scanning a QR code for verification);
- imposing access controls (e.g. a PIN code) for the users of the messaging app;
- using messaging apps with end-to-end encryption only.
- choosing a messaging app which uses encryption on the basis of verifiable open-source technology that has undergone a security audit;
- verifying whether the storage location on the smartphone is protected and stored data (e.g. photos, encryption keys, messages) are encrypted;
- using a messaging app which automatically deletes messages after a period of time;
- choosing a messaging app which never stores data, or deletes the data from the server as soon as the message has been delivered;
- using authorisation management for chat groups.

App blocking is labour-intensive and ineffective

Blocking messaging apps on smartphones is not an adequate security measure. New messaging apps are released on a daily basis and the blocking of unsafe messaging apps consumes a lot of resources. Using a thoroughly screened messaging app is more effective than attempting to block all messaging apps.

Think about how to disseminate the app.

It is important to devote sufficient attention to the implementation of the desired messaging app, so that employees are encouraged to use it. Facilitate a smooth roll out of the chosen messaging app within your organisation. For instance, you may want to consider offering the app for free, accompanied by instructions for its use, or 'pushing' the app to the smartphones of staff. This enables you to implement the app with the correct security settings for immediate safe use.

Action perspective

- Conduct a risk assessment to determine whether a messaging app is the right communication tool for your organisation.
- Check your existing security policy, assess whether it covers the use of messaging apps and update it if required.
- Focus your research on those messaging apps which come closest to complying with your internal security policy.
- Analyse the potential risks and necessary follow-up actions when choosing a messaging app.
- Compile a list of the risk scenarios that apply to your organisation.
- Identify the security measures that have already been implemented in the messaging app of your choice.
- Assess the effectiveness of these measures.
- Identify measures which are missing and/or ineffective.
- Determine the level of residual risk.
- Accept residual risks or take further action to mitigate them.

Finally

Your organisation is responsible for managing the risks involved in the use of messaging apps for business communication. The number of messaging apps is on the rise and their use continues to grow. It is vital to identify the risks involved in the use of messaging apps within your organisation. You must take organisational and technical measures based on your internal security policy. Employees will use messaging apps more sensibly if they are aware of the risks. The use of messaging apps within your organisation must not result in violations of privacy, data breaches or corporate espionage.

Choose your messaging app wisely!

Publication

National Cyber Security Centre (NCSC)
P.O. Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31(70) 7515555

More information

www.ncsc.nl
info@ncsc.nl
[@ncsc_nl](https://twitter.com/ncsc_nl)