Snoop protection

Just how secure is your messaging app? **Ros Page** finds out

Prime Minister Malcolm Turnbull and many of his Canberra colleagues are reportedly fans. Millions around the world use them for everyday communicating, and many people are now turning to secure platforms in light of our metadata retention regime and widespread government internet surveillance.

Messaging on our phones was once a matter of sending simple 160-character messages spelt out with two fingers that required a lot of multiple key pressings, a fair chunk of time and a big load of patience. The message often resembled a kind of abbreviated phonics where 'C U l8r 4 drinks. Thx' was an acceptable way to communicate.

Fast forward to 2017 and, while emojis often take the place of words, we have many more sophisticated (and longer) ways to message each other from our phones.

Messaging by the millions

Messaging apps come in many forms – there's Messenger, a popular spin-off from Facebook, and iOS Messages, which is found on all iPhones. There's also the new breed: WhatsApp, Snapchat and Viber, which have gained millions of users. And in the age of metadata retention and state internet surveillance we've also seen people turn to security-focused apps like Wickr, Confide and Tunnel.

Not everyone wants to use a specialist secure messaging app, preferring instead to stay with something like Messenger that rides on the back of Facebook popularity. We've tested a range of messaging apps to compare their security and usability.

Not all apps are created equal

Typically, when it comes to messaging apps, there tends to be a trade-off between how easy they are to use and their level of security. Although there are no absolute guarantees when it comes to complete security protection, our testing shows that, for general use, there's good security in place with most secure messaging apps. However, there are still some areas for concern, which are not easily solved without reducing usability – for example, if you send a user a picture, they can take a screenshot.

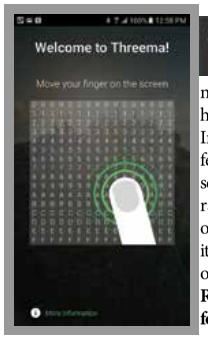
What about all these exploits?

There have been various vulnerabilities, holes, hacks and exploits found in messaging apps in recent years – including those billed as secure apps. So how do these happen? Experts say security code can have small errors and ensuring security is robust against unknown, future flaws can be very difficult. Security audits can find flaws that we know about right now, but there is potential for components to combine in new ways and create exploits in the future. For example, an app may be shown to be very secure, but a new type of video file is released that interacts with the code in an odd way, which then introduces a security bug.

There are also vulnerabilities that can arise if a recipient's device is compromised, say by malware – the end device will decrypt the message and the malware could then view it. Users can also contribute to weak security by using simple passwords and not adopting best practice, such as using two-factor authentication – this is where a password and a security code is required to log in.

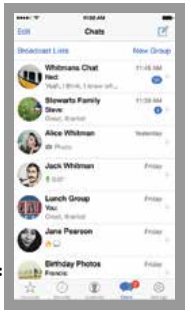
Recommended apps

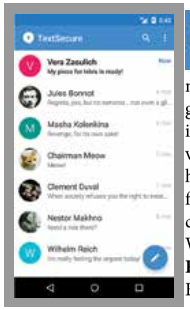
Our list of recommended apps includes security-focused apps as well as others such as WhatsApp, Facebook Messenger and iOS Messages that have wider appeal. The overall score (see table, pp12–13) used to rank the apps reflects the importance of both security and usability in relation to how well a messaging app functions. We suggest choosing an app with an overall rating of 70 or above. On the other hand, if you're more interested in using an app that's simple to get up and running, you can choose one that rates higher in the ease of use criteria.



Threema is fast, easy to navigate, stable and highly responsive. In terms of security features, it ranks second highest and ranks highest overall because of its excellent ease of use score. **Recommended for:** Personal use

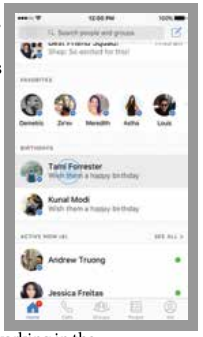
WhatsApp default security settings are very good, as every message is encrypted automatically. Users receive notifications if anything is wrong and it's built on the same protocol as Signal, although it's not fully open-source. We recommend it because it has a good security features score and a very good ease of use score. **Recommended for:** Personal use





Signal can be set up to delete messages after a given time and includes encrypted voice chat. Signal has a slightly lower feature score, so it comes in just under WhatsApp. **Recommended for:** Business/personal use

iOS Messages is built into every iPhone and is completely seamless. If the text bubble is blue, it's being sent securely. It's limited to Apple devices and is closed source, so we just have to trust Apple when it says messages are secure. We've given it an excellent score for ease of use. **Recommended for:** Personal use



Messenger is easy to use and connects you with all your Facebook friends. You can make video calls as well as normal calls. The terms and conditions allow Messenger to record the calls without even knowing the user. Battery usage can be an issue because the application is always working in the background. It uses around 100MB of space on a phone. It scores lower for security features, but an excellent ease of use score earns it a spot on our recommended list. **Recommended for:** Personal use

Wickr doesn't allow screen shots and has multiple layers of encryption. It can't be synced with multiple devices. It has a good security features score and a good ease of use score with an OK rating for features, which sees it at the lower end of our recommended list. **Recommended for:** Personal use ▸

HOW WE TESTED

How secure is it?
We rated the security of your message when it's on your phone, on its way to your contact and on your friend's phone, including how it's stored at both ends. The apps that rate highest for security fulfill more of the security features criteria. These include encryption, amount of user data collected, server location and protection. They also include protection from messages being copied/forwarded, message destruction, security audit and if the code is open-source.

How easy is it to use?
The ease of use score is given based on the app's clarity and usability in performing messaging in a secure way. Apps that have confusing security settings score lower, as do apps that are difficult to operate. Apps that score highly generally have good secure defaults and clear avenues for altering or improving security.

What features does it support?
The apps are scored for the range of features they have in addition to sending and receiving messages. This includes what types of attachments are supported and whether attachments can be saved, what permissions are required to access what files, the type of login, message limits and whether the user can manage data retention, idle time lock, user alert and types of notifications, user typing alert, message previews, support for use on more than one device, whether the user remains logged in and the way the account can be terminated. ■

Recommended	App	Price ($)	PERFORMANCE: Overall score (%)	Ease of use score (%)	Security features score (%)	Versatility score (%)	VERSIONS: Android	iOS	SECURITY FEATURES: End-point encryption	In-transit encryption	Personal encryption key	What user data is collected?	Zero access from vendor (claimed)	Server location	Server data retention time	Government data request policy available	Conversation log encryption	Copying/forwarding messages	Screen shots allowed	Message destruction
✓	Threema	4	78	90	65	53	✓	✓	✓	✓		Basic statistics	✓	Switzerland	na	✓	✓	✓	✓	✓
✓	WhatsApp	0	75	80	70	60	✓	✓	✓	✓		Account info	✓	USA	*	✓	✓	✓	✓	✓
✓	Signal	0	74	80	70	47	✓	✓	✓	✓	✓	na	✓	Distributed by users	na	✓	✓	✓	✓	✓
✓	iOS Messages	0	71	90	45	67		✓	✓	✓		Variety of statistics	✓	USA	na	✓	✓	✓	✓	✓
✓	Messenger	0	70	90	45	53	✓	✓		✓		Facebook related	(A)	Sweden, USA	As needed	✓	✓	✓	✓	✓
✓	Wickr Messenger	0	70	70	70	67	✓	✓	✓	✓	✓	Basic statistics	✓	na	User set	✓	✓	✓	✓	✓
	Confide	0	68	70	65	60	✓	✓	✓	✓		Contacts and basic info	✓	na	**After open	✓	✓		Not in messages	✓
	SnapChat	0	68	70	65	60	✓	✓	✓	✓		Any info entered in app	✓	Worldwide	**After open	✓	✓	✓	✓ (notifies other user)	✓
	Viber	0	67	80	50	53	✓	✓	✓	✓		Account info	✓	Belarus, Israel	As needed	✓	✓	✓	✓	✓
	Chat Secure	0	64	70	55	60	✓	✓	✓	✓		Activity dependent	✓	Can use own server	na	✓	✓	✓	✓	✓
	WeChat	0	62	70	50	60	✓	✓		✓		Personal and shared info	✓	China	na	✓	✓	✓	✓	✓
	Telegram Messenger	0	59	70	45	40	✓	✓	✓	✓		Messages, photos, videos, documents	(A)	Singapore, UK, USA	***As needed	✓	✓	✓	✓	✓
	Tunnel X	0	51	40	65	60	✓	✓	✓	✓	✓	Basic statistics	✓	USA	As needed	✓	✓	✓	Texts no/ app yes	✓
	Silent Text	10	50	50	50	40	✓	✓	✓	✓		Basic statistics	✓	na	As needed	✓	✓	✓	Y	✓

App	No metadata collected	Message storage location	Security audit	Open-source	MESSAGING FEATURES: Supports multimedia attachments	Can attachments be saved?	Permission to access what files?	Login (username and password)	No message limits	User-managed data retention	Idle time lock	User alert and notification types	Message previews	Multi-device support	Always logged in	Account termination (delete)
Threema	✓	Device	Internal		✓	✓	Contacts, photos, media, files	Threema ID	✓	✓		✓	✓	✓	✓	✓
WhatsApp	✓	Device	Internal		✓	✓	Contacts, photos, media, files	Phone number, country	✓	✓		✓	✓	✓	✓	✓
Signal	✓	Device	Independent		✓	✓	Device and app history, identity, calendar, contacts, location, SMS, phone, photos, camera	✓	✓	✓		✓	✓	✓	✓	✓
iOS Messages	✓	na	na		✓	✓	Photos, contacts, media, audio, location, microphone	No login	✓	✓		✓	✓	✓	✓	✓
Messenger	✓	Server	na		✓	✓	Calendar, camera, contacts, locations, microphone, phone, SMS, storage	✓	✓	✓		✓	✓	✓	✓	Deactivated
Wickr Messenger	✓	na	Independent		✓	✓	Contacts, photos, media, files on device	Two-factor authentication	✓	✓		✓	✓		✓	✓
Confide	✓	na	External		✓	✓	Photos, media and files, make phone calls, location, contacts	✓	✓	✓		✓	✓	✓	✓	✓
SnapChat	✓	Not stored	Internal		✓	✓	In-app purchases, identity, contacts, location, SMS, phtotos/media/files, camera, microphone, Wi-Fi details	✓	✓	✓		✓	✓	✓	✓	✓
Viber	✓	na	na		✓	✓	In-app purchases, device and app history, identity, contacts, location, SMS, phone, photos/media/files, camera	Phone number	✓	✓		✓	✓	✓	✓	Deactivated
Chat Secure	✓	na	Independent	✓	✓	✓	Identity, photos/media/files, Wi-Fi details, device ID, call information	PIN and/or image key	✓	✓	✓	✓	✓	✓	✓	✓
WeChat	✓	na	Independent		✓	✓	Photos, media, files, phone calls, location, contacts	Name, mobile number and password	✓	✓		✓	✓	✓	✓	✓
Telegram Messenger	✓	Server	na	(B)	✓	✓	Contacts, photos, media, files on device	✓	✓	✓		✓	✓	✓	✓	Deactivated
Tunnel X	✓	na	na		✓	✓	USB storage, network connections	PIN, nickname	✓	✓		✓	✓	✓	✓	✓
Silent Text	✓	na	na	✓	✓	✓	Phone calls, pictures, video, audio, contacts, photos, media, files	✓	✓	✓		✓	✓		✓	Delayed

USING THE TABLE Recommended We recommend products with an overall score of 70% or higher. **Price** Price paid in May 2017. **Overall score** Based on the weighted ease of use (55%), security features (40%) and versatility/features (5%) scores. **Ease of use score** Based on tests performed by the tester. **Security features score** Based on a checklist of tests performed by the tester. **Versatility score** Based on what the program can do/features it supports. **What user data is collected** *Basic details* Information to provide a profile for the user, such as their name, email address or mobile number. *Basic statistics* General usage information without any detailed intrusive information like reading messages. Counting messages is included in basic statistics. **Security audit** If and how the app's source code is checked for bugs or vulnerabilities. **Open-source** is where the source code is available publicly. **App permissions required** For access to each of these files on the device. **Login type (username and password)** Does the login require identification beyond password such as two-factor authentication. **Message limits** The number of characters. **User managed data retention** Can the user manage the data retention. **Idle time lock** Locks when not in use. **User alert and notification types** Available or not. **Message previews** Are previews shown in the Android drop-down menu, for example. **Multi-device support** What number of concurrent devices are supported at the same time. **Always logged in** If user needs to re-login. **Account termination** If you log back in, you get a "new" account. **Deactivated** If you log back in, you reactivate your account. **Delayed** The account is scheduled to be deleted, but not immediately. **TABLE NOTES (A)** CHOICE was able to test and confirm. **(B)** Telegram expected to release full code shortly. **na** Information not available from vendor. * WhatsApp messages not stored on server. ** After messages are opened they're deleted. *** Secret chats deleted on Telegram, other data as needed.