How Secure Is Your Messaging App?

Here’s how to tell whether your private messages could be hijacked or whether they’re safe from prying eyes.

December 27, 2018 7 min read

This story originally appeared on PC Mag

Which messaging app would you choose for absolute security? Every developer will profess that they responsibly consider the security and privacy of their users. But with so many different choices, it can be hard to tell which messaging platforms you can trust.

This set of criteria can help you evaluate the security of your messaging apps and decide how far you can trust them.

Encryption

Virtually no messaging app sends your messages in clear text format; all platforms use some form of encryption to scramble messages and prevent unauthorized parties from reading them. But not all forms of encryption are equally secure.

Some apps encrypt your messages in transition and storage, but also hold a copy of the encryption keys. This means they can decrypt and read the content of your messages. Companies that use this form of encryption usually do so to mine user data for advertising purposes. Examples include the soon-to-be-phased-out Google Hangouts, Skype, and WeChat.

Related: Security Trends Your Company Needs to Embrace in 2019

But if the servers of these companies fall victim to a data breach, malicious actors will gain access to the keys and can also decrypt your messages. The companies that host these services are then open to warrants from government agencies that want to investigate users' private communications.

The most secure platforms employ end-to-end encryption (E2EE). These apps use public key cryptography to encrypt messages: For each user, the platform issues a pair of public and private encryption keys. It stores the public keys on its servers, but private keys are stored on user devices only.

Users can retrieve one another's public keys from the servers to encrypt their messages. Each message encrypted with a public key can only be decrypted with its corresponding private key, which is in the exclusive ownership of the recipient. End-to-end encryption ensures that not even the company that hosts the application can access a message's content. Even if hackers break into their servers or three-letter agencies force them to hand over user data, they won't be able to decrypt the content of messages.

At present, more and more platforms are adopting end-to-end encryption. Some examples include Signal, WhatsApp, Wickr, and Apple's iMessage.

Other messaging apps such as Telegram and Facebook Messenger also support end-to-end encryption, but it's not turned on by default. You have to enable the feature manually for individual chats. Skype also recently added a feature called Private Conversation that provides end-to-end encrypted chat, but it also is not the default configuration.

Message Deletion

Although end-to-end encryption protects you against eavesdroppers, it's of no use if your device or the devices of the people you chat with fall into the wrong hands. Another

security feature to look for in messaging apps is the ability to remove messages after they're sent. Deleting messages ensures that if one of the devices becomes compromised, your sensitive communications aren't exposed.

Related: What's Happening on The Entrepreneur Index Right Now

Telegram, Signal, and Skype let users delete messages for themselves and the recipients of their messages. Wickr also has a "recall message" feature, which deletes messages from the devices of everyone involved in a conversation. And WhatsApp added a "delete for everyone" option last December, but you can use it to delete only those messages you've sent within the last 13 hours.

iMessage doesn't support the deletion of individual messages: You can delete only entire chats, and when you do so, you're removing a chat only from the device you're using; it stays on all other iOS devices that share the same Apple ID as well as on the devices of the person you were chatting with.

A convenient addition to deletion is the self-deleting message. This feature will automatically remove messages from the devices of all users after a certain amount of time expires. On Signal, it's called "disappearing messages." When you turn on the feature, you specify an expiration time after which a message is automatically removed from all devices.

Wickr's self-destruct feature is called "Burn-on-read." Telegram and Facebook Messenger also support self-destructing messages but only for their secret chat features that run on end-to-end encryption. WhatsApp doesn't support self-deleting messages.

Note that if the receiver of a message takes a screenshot of your chat and stores it elsewhere, deletion will be pointless; message deletion won't protect you against malicious conversation partners. Rather it's a safeguard against unintentional mistakes.

Metadata

Along with the content of messages, you should be concerned about metadata—the information that a messaging platform stores about your activities. Metadata includes sender and receiver IDs, the time a message is sent, login times, IP addresses, device types, duration of calls, and other information that can reveal your identity and habits.

Related: The Dangers of the Internet of Things (Infographic)

In the wrong hands, metadata can be very harmful, because it can reveal a user's communication patterns: the people they're in contact with, their geographical location, the timing of their messages, and more.

Most popular messaging applications collect a wealth of information about user activity. But Signal has the best track record, since it registers only the phone number with which you created your account and the last date you logged in to your account (not including the hour, minute, and second).

Transparency

Beyond the promises of developers, independent experts should be able to verify the security of a messaging application. Open-source platforms – applications whose developers make the source code available publicly – are generally more reliable, because they usually undergo thorough peer review and cross-examination by other developers and security experts.

Signal is open-source, and the source code of all versions of the app is available for download on GitHub. Wickr made its source code publicly available last year. Telegram also provides the source code of its apps and lets developers create and publish their own versions of the client app that can hook into its application programming interface (API).

Related: Google Home and Amazon Echo Can Store Your Voice Recordings. Here's When They Could Be Used Against You.

WhatsApp and Facebook Messenger are not open-source, but they do use the open-source Signal Protocol to encrypt users' messages.

Closed-source apps such as iMessage require users to fully trust the developer to check its code for security bugs and not to install backdoors: intentional vulnerabilities meant to provide select parties (say, advertisers and government agencies) access to encrypted message content.

Nothing's Perfect

To sum up, when you're evaluating a messaging app, ask yourself these questions:

- Does it use end-to-end encryption?
- Does it allow message deletion for all parties to a conversation?
- How much metadata does it collect?
- Is the source code open for review, and have outside experts confirmed its security?

Answering them will give you a good sense of how secure a messaging app is.

But to be clear, there's no such thing as absolute security. And even the most secure messaging platform won't protect you against yourself.

In addition to choosing a secure messaging app for your sensitive communications, you should develop personal safety habits such as setting a screen lock on your devices, not installing apps from unknown developers, and not oversharing

online. The best way to have a private conversation is to avoid online platforms altogether.

https://www.entrepreneur.com/article/325395