# How to Keep Your Emails and Texts Private

## Some smartphones feature end-to-end encryption, but experts prefer third-party apps

by Ed Waldman, **AARP**, May 2, 2022

Russian dissidents have to make sure their emails and texts are private and encrypted. So do government whistleblowers. And so might you.

At the very least, you want to make sure that any emails or texts you send are protected.

A number of free email and text services use end-to-end encryption to ensure the privacy of messages. End-to-end encryption means that only you and the person you are communicating with can read your message — no one in between can see it.

“Think of it as a pipe between the two devices,” says Christopher Budd, director of threat research for Sophos. The internet security firm is based in the United Kingdom. “When you have it, what is passing in the pipe between the two devices is encrypted. But what is on both of the devices in unencrypted.”

Android and Apple devices also have settings users can deploy to limit what third parties, especially marketers and advertisers, can learn about them from their email activity.

## iPhone and Gmail privacy tools

Marketing emails are often about more than promoting products. Some allow the senders to glean information about you, such as what emails you open, how long you spend reading them and whether you clicked on any links.

If you have an iPhone, you can prevent this by turning on Mail Privacy Protection. When activated, this setting hides your IP address, a numeric designation that identifies your device's location on the internet, so senders can’t associate it with other stuff you do online and figure out where you are. It also prevents senders from seeing if you’ve opened any email they’ve sent to you.

To turn on Mail Privacy Protection, go to **Settings | Mail**. Then toggle the **Privacy Protection** button to on.

Android devices don't have anything exactly like Mail Privacy Protection, but you can stop images from automatically loading in the Gmail app. This can help with privacy because many advertisers seed emails with tiny hidden images that report when you open the message.

To stop the automatic download, go to the Gmail app and tap the **Menu icon** (the three lines at the top left). Choose **Settings** — you may have to scroll far down; it’s nearly at the bottom — then tap **your email address.** In the Images area, enable **Ask before displaying external images (also displays dynamic email).** Dynamic email lets you complete tasks — replying to an invitation, for example — from within the message.

## Private email services

If you want to go take email security to the next level, you can use a free email service like ProtonMail or Tutanota that uses end-to-end encryption.

Engineers and scientists from the Massachusetts Institute of Technology and the Geneva-based European Organization for Nuclear Research (better known as CERN, from the French acronym for its original name) built ProtonMail. Its servers are buried under a kilometer of granite in Switzerland, and the service is protected by Swiss privacy law.

You don’t need to provide any personal information to create a ProtonMail account. The ProtonMail app is available for both iOS and Android devices, but if you prefer not to install software, you can access your account via web browser by going to the ProtonMail site.

Tutanota is based in Hanover, Germany, and its name, derived from the Latin words *tuta* and *nota*, means secure message, according to the company’s website. Emails that pass through the service are protected by the German Federal Data Protection Act, which bans the collection of personal data without permission.

Tutanota encrypts your subject line, something ProtonMail doesn’t do. Its app is also available for both iOS and Android.

Other services that offer encrypted emails include Hushmail, Mailfence and PreVeil.

## Encrypted text messaging

In the olden days — a year or two ago — text messages sent through your cellular provider were not encrypted. It was best not to text your bank account number or any password to a family member or friend. Not only could bad actors easily intercept texts, your provider could see the messages you sent and received, and store that information in their systems.

But today, if you have an iPhone, iPad or Mac and use Apple’s Messages app to send your text to another iPhone, iPad or Mac, your message is encrypted. And if you’re not in the habit of deleting your texts, you can ensure that messages stored on iCloud, Apple’s cloud storage service, are also encrypted by enabling two-factor authentication, a security process that requires two steps in order to verify a user — a password and a texted code number, for example.

Android also has recently adopted end-to-end encryption for messaging from one user of its operating system to another, but it’s not universal. “The thing with Android is it depends on the version you have, the [phone] manufacturer and on your carrier,” Sophos’ Budd says.

According to Google, which makes the Android OS, messages should be encrypted if both you and the person you’re communicating with have the latest version of Google’s messaging app and have enabled its chat features. To check this, tap the app’s **Menu icon** (the three vertical dots in the upper right corner) **| Settings | Chat features** and see if **Enable chat features** is toggled on.

If you see a lock icon on the send button and next to message time stamps, that means your conversation is encrypted.

## Third-party services

If you have an iPhone and your best friend (or confidential source) has an Android, all is not lost. You can still send encrypted messages by using a third-party service. A number of options are free, among them Signal, Telegram and WhatsApp. All have end-to-end encryption and are available for Android and iOS.

“Most security people I know prefer Signal,” Budd says. “There are a couple of reasons. First, it was built to be secure from the very beginning. It’s also about the message storing. WhatsApp is owned by Facebook,” which has had problems with data privacy in the past.

Budd says many in the security industry don’t trust Telegram as much as they trust Signal because Telegram is hosted in the United Arab Emirates, “so there are questions and concerns around data protection and civil liberties.

“These concerns are always present when we talk about end-to-end encryption because the servers are an end,” he says. “And information can potentially be obtained via court order or other law enforcement or government action.”

To set up Signal on your device, download the app from the Apple App Store or Google Play, open it, enter your mobile number and tap **Continue.** This triggers the service to text you a code. Enter it in the app, then enter your first name, which is required (you can also give your last name, but that’s optional). Tap **Save,** create a PIN and tap **Next.**

The directions for setting up WhatsApp or Telegram after downloading are very similar — the order changes a little, but you’ll need to enter the same information for all three apps. And remember that they don’t work with each other. You can send a Signal message only to another Signal user. They can’t get your Signal message on their WhatsApp account.

*Ed Waldman is a contributing editor and writer who covers technology. He previously was an editor at the* Baltimore Sun, *taught journalism at the University of Maryland and launched a statewide high school sports website.*