From: <https://betterhumans.pub/how-to-communicate-privately-in-the-age-of-digital-policing-cf78ff2a79a7>

By:David Koff

Date:May 9, 2019·21 min read

**How to Communicate Privately in the Age of Digital Policing**

Your best options for keeping your messages and email private and secure



Even non-spies need privacy. Let’s talk about how. Photo courtesy of [Pixabay](https://pixabay.com/en/secret-top-stamp-spy-army-3037639/).

Introduction: A Simple Conversation

Let’s say that you’re sitting in your living room in your London flat and chatting with a dear friend. You’re discussing something personal and maybe even a bit scary: your doctor has noticed something unusual on your skin and wants to run a biopsy to test for cancer. Your friend sits with you, listening, while you get emotional about how the mere *mention* of the word cancer is making you angry, sad, worried, and nervous. You describe how a diagnosis of cancer might impact your career, your earning potential, your social life, your relationship with your significant other and more.

Do you have, sitting there in your living room, the right to a private conversation? *Of course, you do.* Do you have concerns about whether your conversation on a private and personal matter is being overheard by others and, perhaps, being used against you? Of course, you don’t: it’s a private conversation in a private setting.

But now let’s now say that you’re having the very same conversation with the very same friend while you sit in the very same living room in London. Only now, let’s imagine that your friend is sitting in *her* living room in Mumbai, where she lives. As a result of the distance, let’s say that you’re having the long-distance conversation via a phone call, a video chat app, or text messages.

Do you have, while using this technology, the same right to a private conversation? *Of course, you do.* Do you have concerns about whether your conversation on a private and personal matter is being overheard by others and, perhaps, being used against you? Unfortunately… the answer to that question isn’t as clear in today’s massively interconnected world.

Privacy and security experts would caution you — and rightly so — to think about what it is that you’d like to communicate *before* you do the communicating, and then choose the best tools to make that communication as secure and private as you’d like it to be. **How to implement this** approach is what we’ll be discussing today, so let’s jump right in.

The Three Canaries

Some of you may be thinking, “What’s all the fuss, [brah](https://www.urbandictionary.com/define.php?term=brah)? I’m cool with sending text or SMS messages; I’ve got no problems chatting with my [peeps](https://www.urbandictionary.com/define.php?term=peeps) via Facebook, Twitter, and other social media platforms; Slack is [totes](https://www.urbandictionary.com/define.php?term=Totes) fine for live-chatting with my colleagues; and I still believe in using old-fashioned email, the [nearly 50-year-old](http://bit.ly/HistoryOfEmail) technology that never lets me down!”

I get it. All of the messaging options I just mentioned are readily available and easy-to-use. Unfortunately, they’re also considered insecure for important reasons which I’ll refer to as “The Three Canaries”:

1. All technology is hackable. Yes, [cell networks too.](https://blog.kaspersky.com/hacking-cellular-networks/10633/)
2. Few companies, if any, can be trusted with your personal data.
3. Every company can be ordered to disclose the data they’ve kept about you to law enforcement and/or government authorities.

For some eye-opening statistics, check out the transparency disclosures — all linked below — from [Amazon](https://d1.awsstatic.com/certifications/Information_Request_Report_June_2018.pdf), [Facebook](https://transparency.facebook.com/government-data-requests), [Twitter](https://transparency.twitter.com/en/information-requests.html), [Snapchat](https://www.snap.com/en-US/privacy/transparency/), [Microsoft](https://www.microsoft.com/en-us/corporate-responsibility/lerr), [Apple](https://www.apple.com/legal/transparency/), and [Google](https://transparencyreport.google.com/user-data/overview?hl=en). You’ll notice three trends if you parse these data: first, the number of requests from government and law enforcement for your personal data grows every year; second, technology companies comply with these requests most of the time; third, The United States — that beacon of freedom! — issues more requests for user data than every other country. By a huge amount. 👈

Sigh.

Digital tools to the rescue

Fear not, citizen! There are *always* tools available to help us achieve our legal goals, and this situation is no different. In our case, to lessen or eliminate The Three Canaries, we should only use secure messaging solutions that offer end-to-end encryption (or “E2EE” if you like sounding fancy).

E2EE, used most often with secure messaging systems, is a method of encrypted communication where only the communicating users — just the sender and the receivers — can read the messages. When users employ E2EE, the Internet Service Providers, cellphone companies, oppressive governments, private investigators, spy agencies, or even the companies providing the E2EE service cannot view the contents of your encrypted messages.

To understand why E2EE is so important, let’s go back to your living room and the conversation with your dear friend about your health. Now, let’s view that same conversation through the lens of The Three Canaries:

1. **All technology is hackable.**If servers along the transit path of your E2EE messages are hacked and your messages are intercepted, you're still safe: all of your messages are *still* encrypted and, therefore, impossible to see by prying eyes.
2. **Few companies can be trusted with your personal data.** If you rely on E2EE technology when sending your messages, then even the companies hosting that technology cannot read your messages. Therefore, those companies won’t have access to your personal information, beyond the email address or phone number you may have provided when signing up.
3. **Every company can be ordered to disclose data.** If the most powerful intelligence agency on the planet — the CIA — were to subpoena the provider of your E2EE messaging service and force them to turn over your messages, you’d still be safe. That’s because the provider would only be able to hand over encrypted messages. And, as late as 2017, we have proof that [the CIA cannot crack the encryption of messages which use E2EE](https://www.wired.com/2017/03/wikileaks-cia-hack-signal-encrypted-chat-apps/).

Now we’re getting somewhere. We’re taking back some of the privacy that’s been removed from our control. With that in mind, let’s review the best options available for secure messaging and email.

Please note: in nearly every case, I’ll be highlighting the (Apple) iOS version of each solution. There’s a reason for that: [Apple’s iOS is — by far — safer than either Microsoft’s Windows or Google’s Android](https://www.cnbc.com/2015/02/27/5-billion-android-apps-open-to-hack.html). These results have been [confirmed](https://www.pandasecurity.com/mediacenter/mobile-security/android-more-infected-than-ios/) by others. [Repeatedly](https://us.norton.com/internetsecurity-mobile-android-vs-ios-which-is-more-secure.html). And then [again](https://twitter.com/SecX13/status/968225118517452800). And then [again](https://krebsonsecurity.com/online-banking-best-practices-for-businesses/). [I looked at these references. –FNC]

You might not like that, but thems the facts, kiddo. And if we’re going to focus on secure communications, then we’ll need to take the entire OS into consideration as well, not just the apps that run on them.



Photo by [Dayne Topkin](https://unsplash.com/@dtopkin1?utm_source=medium&utm_medium=referral) on [Unsplash](https://unsplash.com/?utm_source=medium&utm_medium=referral)

Secure Messaging

For our purposes, I’ll define a message as “a short note or picture which is digitally transmitted via some method other than email”. For any messaging service to be considered secure, it must demonstrate — at the very least — that:

* it encrypts both your messages *and* your attachments
* it uses top encryption standards and turns on that encryption by default
* it encrypts all meta-data (all other data embedded in your message and in its transmission)
* it is independently funded
* it never collects customer data
* it’s been recently audited (or code-checked) by third parties

BONUS if the software is 100% open source and offers self-destructing messages.

After reviewing the list above and comparing those needs against[a comparison of all messaging services on the market](https://www.securemessagingapps.com/), **there are — it turns out — only three substantive choices when it comes to picking the most secure messaging services.**

Signal is largely considered the best, while

Threema and

Wire are both considered excellent as well.

Signal



The Signal logo.

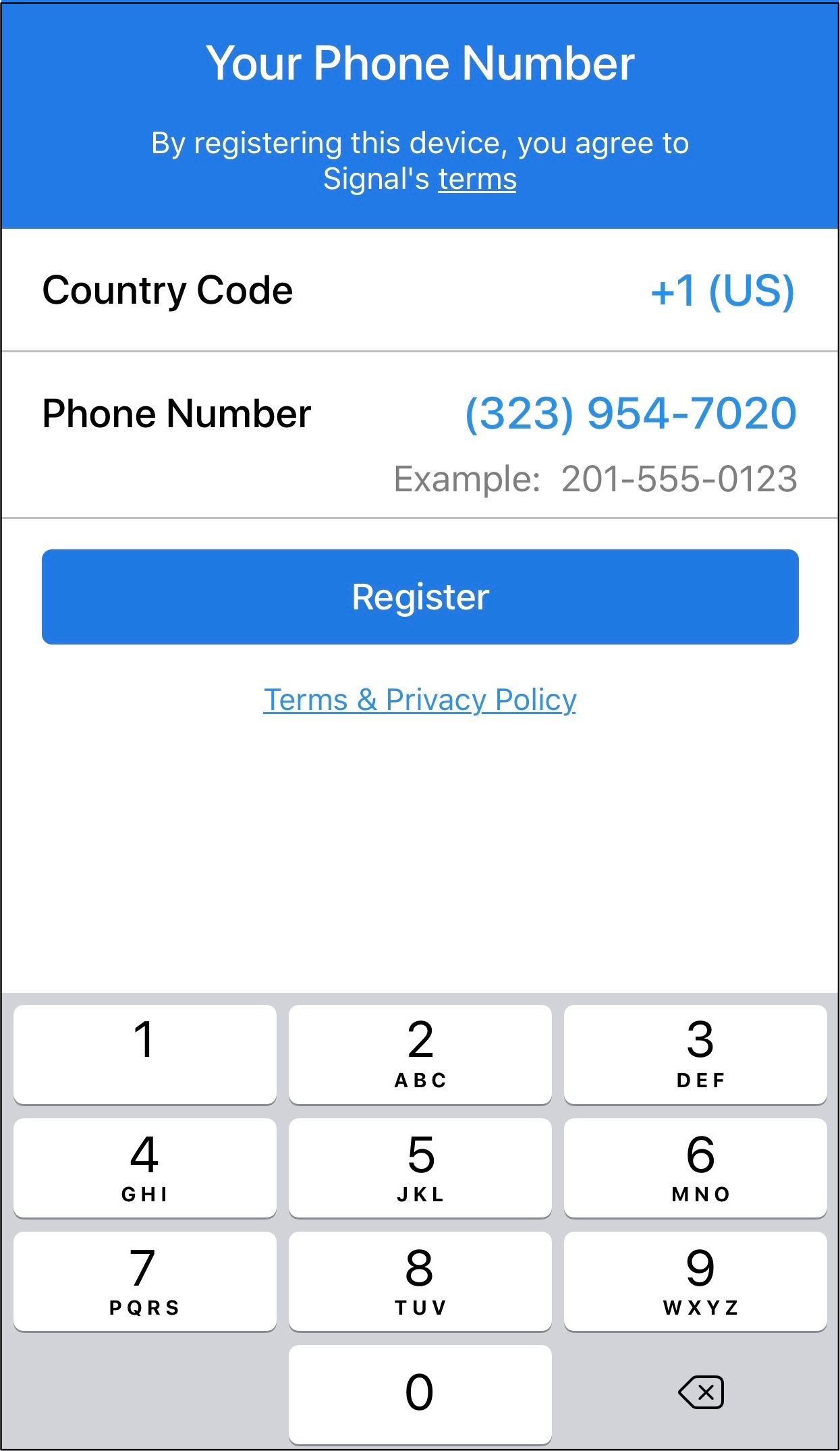
Signal is the top secure messaging choice for most security professionals and for popular technology websites like [Wired magazine](https://www.wired.com/story/ditch-all-those-other-messaging-apps-heres-why-you-should-use-signal/). It’s easy to use, very secure, and — unlike most of the other messaging options — it was designed to be an entire end-to-end platform, not just an application. In fact, Signal’s technology, also known as [the Signal Protocol](https://en.wikipedia.org/wiki/Signal_Protocol), was adopted by WhatsApp, so it’s now become the de facto standard for the majority of secure messages sent on the planet. That’s billions of secure messages sent every day — pretty amazing. What’s also amazing is that Signal brings their E2EE to your messages, phone calls and — get this — your video chat. Yup! As long as all parties are using Signal, the app will protect literally everything that you communicate with E2EE.

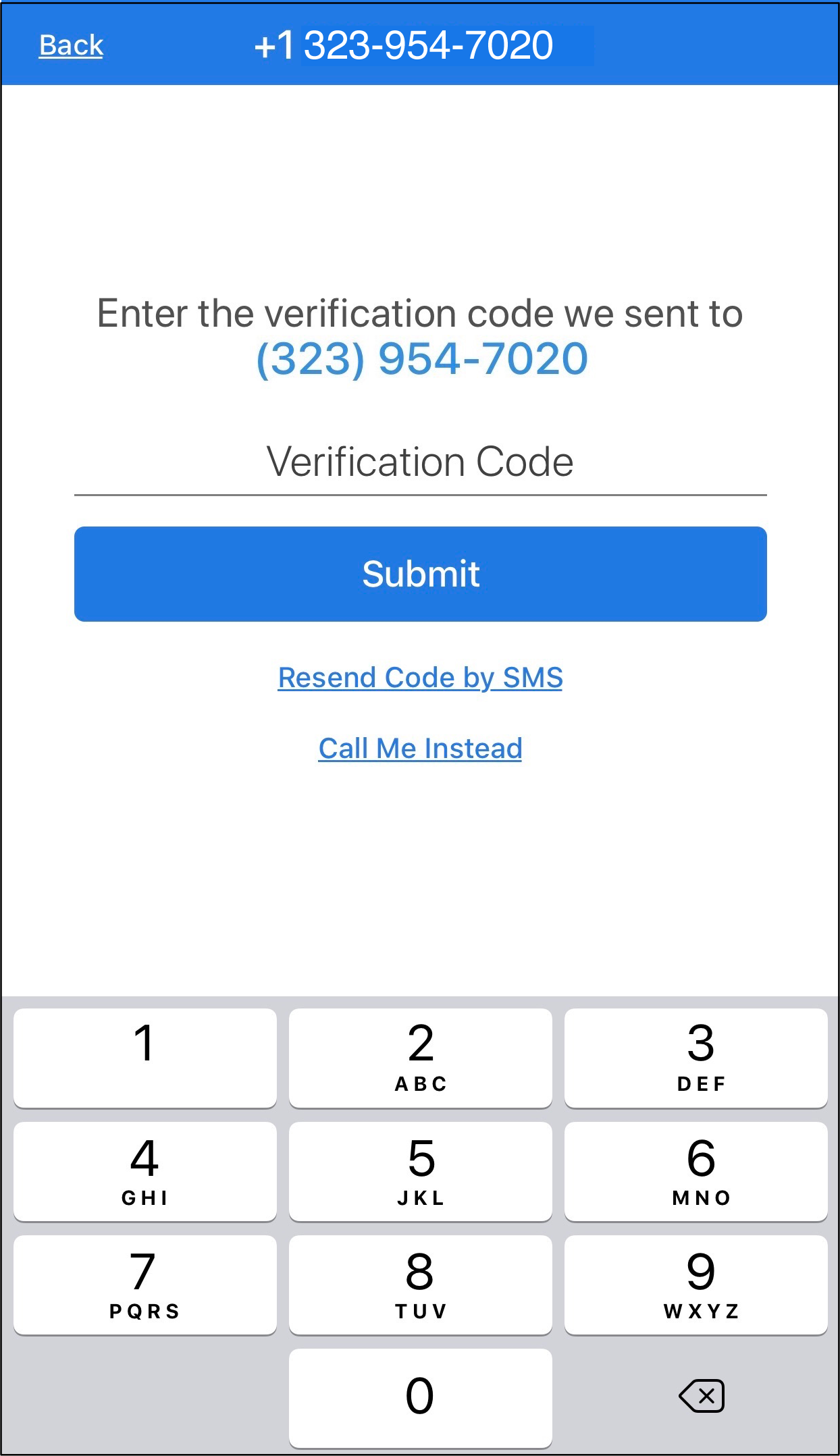
I never say this — literally, never — but to get started with Signal, you should [read the company’s privacy policy](https://signal.org/legal/). I know, I know: it sounds like I’m asking you to poke your eyeballs out with a butter knife, but trust me. It’s only a few paragraphs long, and its worth reading because of how nice it is to see a company caring about your privacy.

**Setting it up**

[Download the app](https://signal.org/download/) for iOS (avoid using the desktop versions, please—more on that below) and launch.

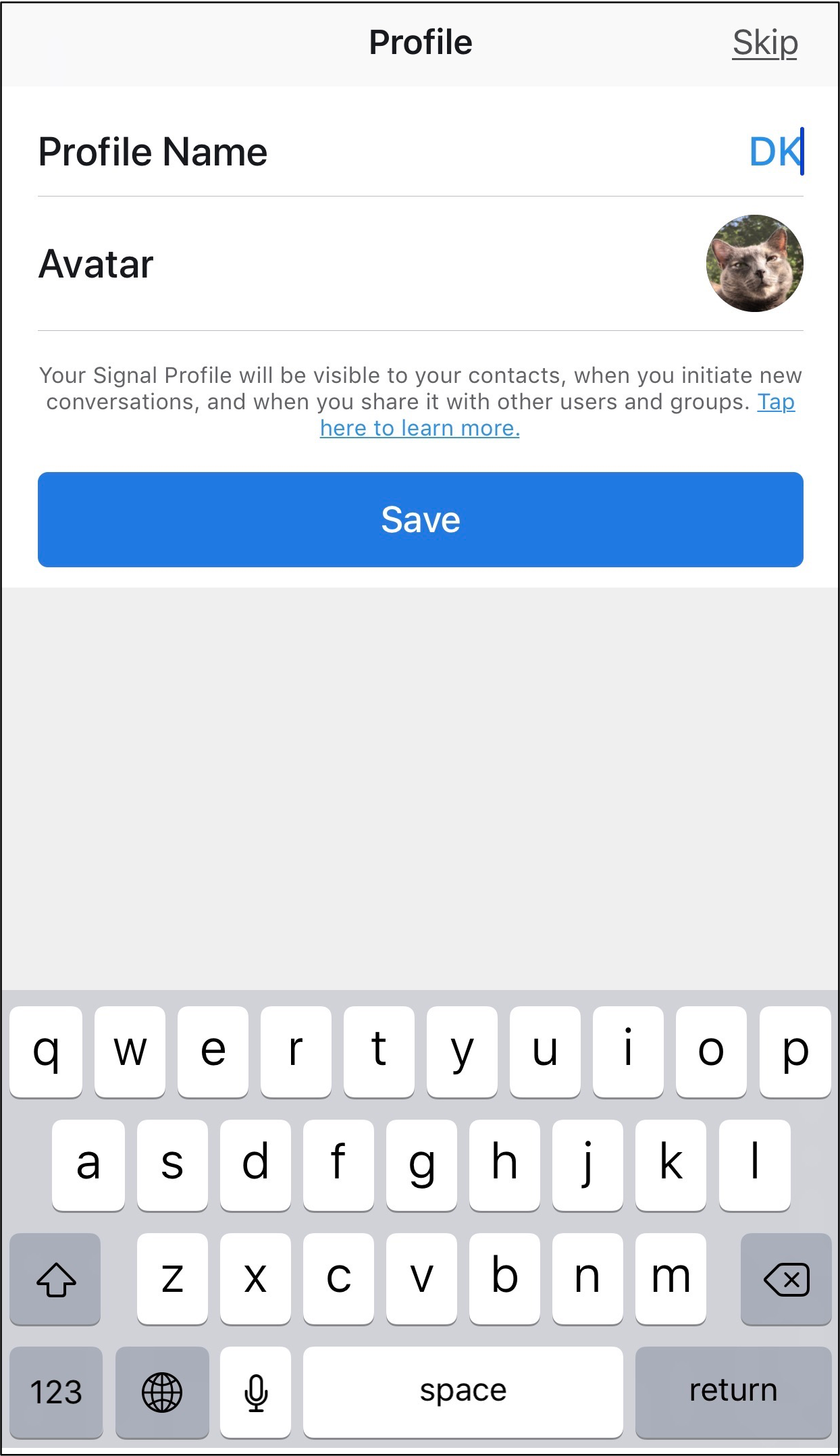
On the first launch, Signal asks you to provide a phone number as shown below, at left. Enter any valid phone number you have and remember: this doesn’t have to be and *probably shouldn’t be*your actual cell phone number (more on that below under “[Caveats](https://betterhumans.pub/how-to-communicate-privately-in-the-age-of-digital-policing-cf78ff2a79a7#b400)”). When you click “Register”, Signal sends a confirmation code to the phone number you provided. Enter the six-digit code they’ve sent by text message on the screen, at right, and click “Submit”.





Signal’s setup and verification process. All screen shots by the author.

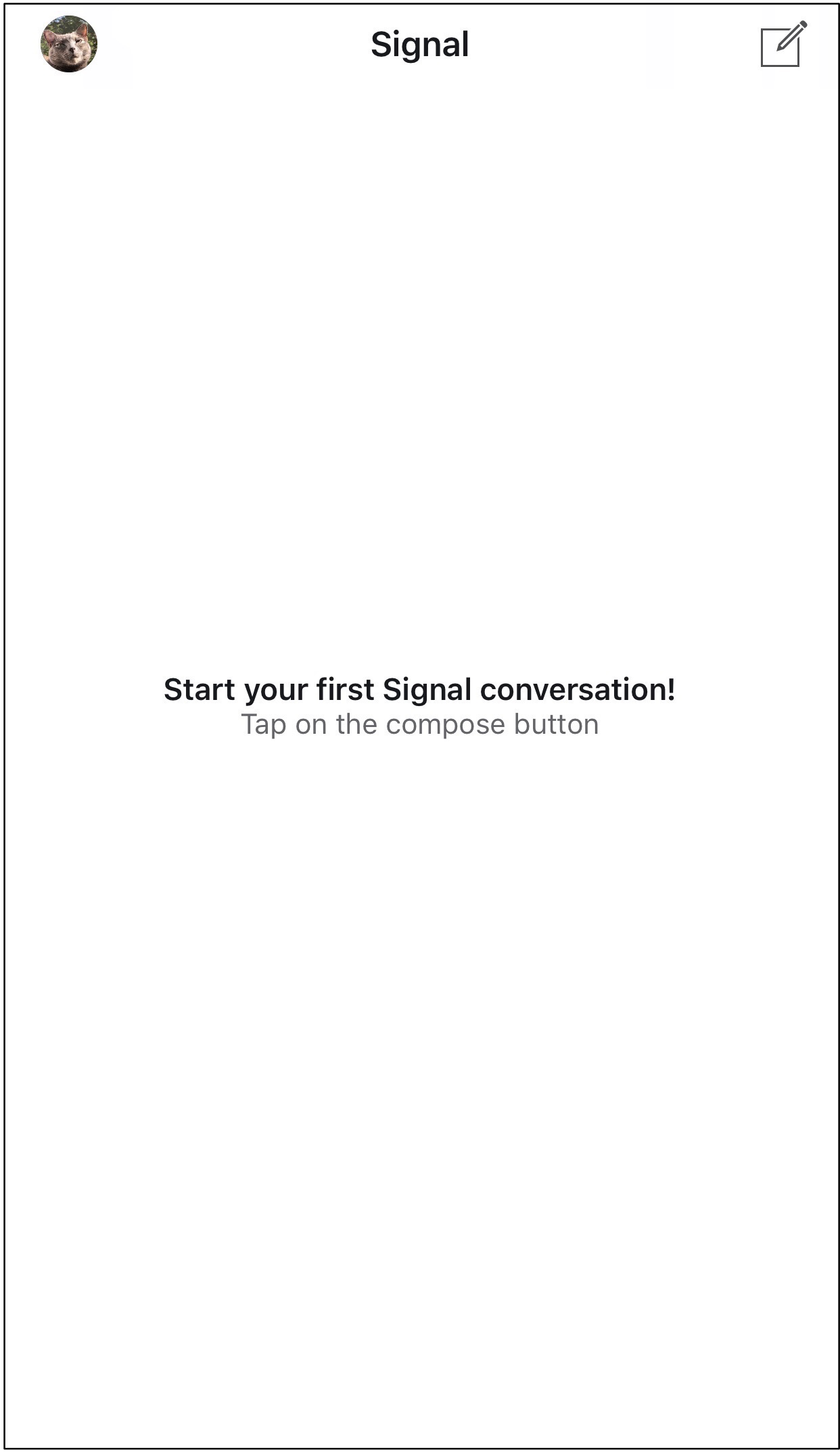
Now, you’ll create a profile name and avatar. You can choose to have this profile easily identify you or not. When you’ve chosen your profile name and Avatar, tap “Save”. Your profile name and picture will be visible to any new contact you add; consider using something familiar to them, so that they’ll recognize you. Conversely, consider using something generic and mysterious if you prefer less name or face recognition. In my case, I chose to use my initials and a picture of a cat that may or may not be the same cat that I did or did not rescue when she was just one-day-old. #Softie

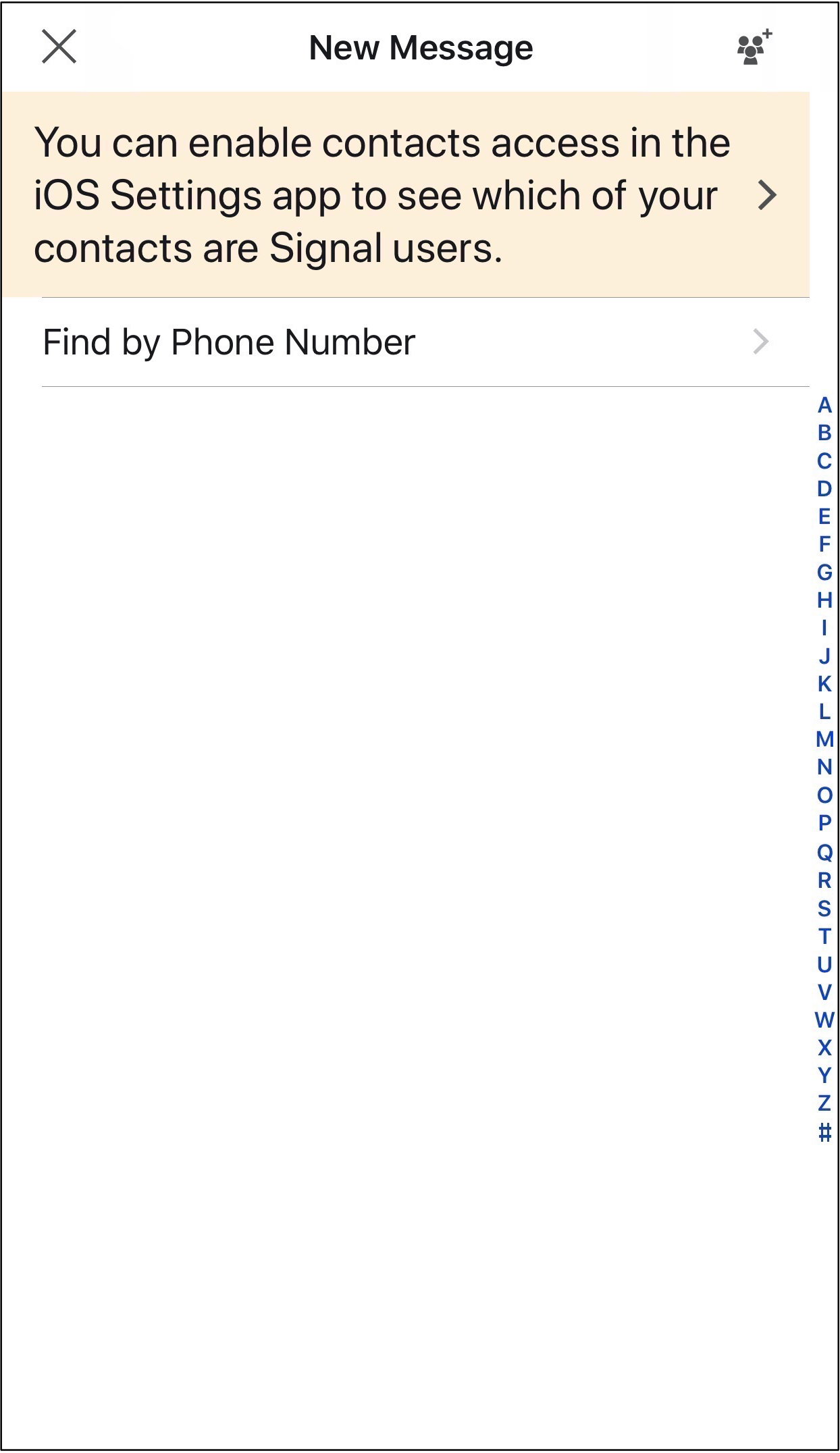


Be as specific or as general as you like here.

Using Signal

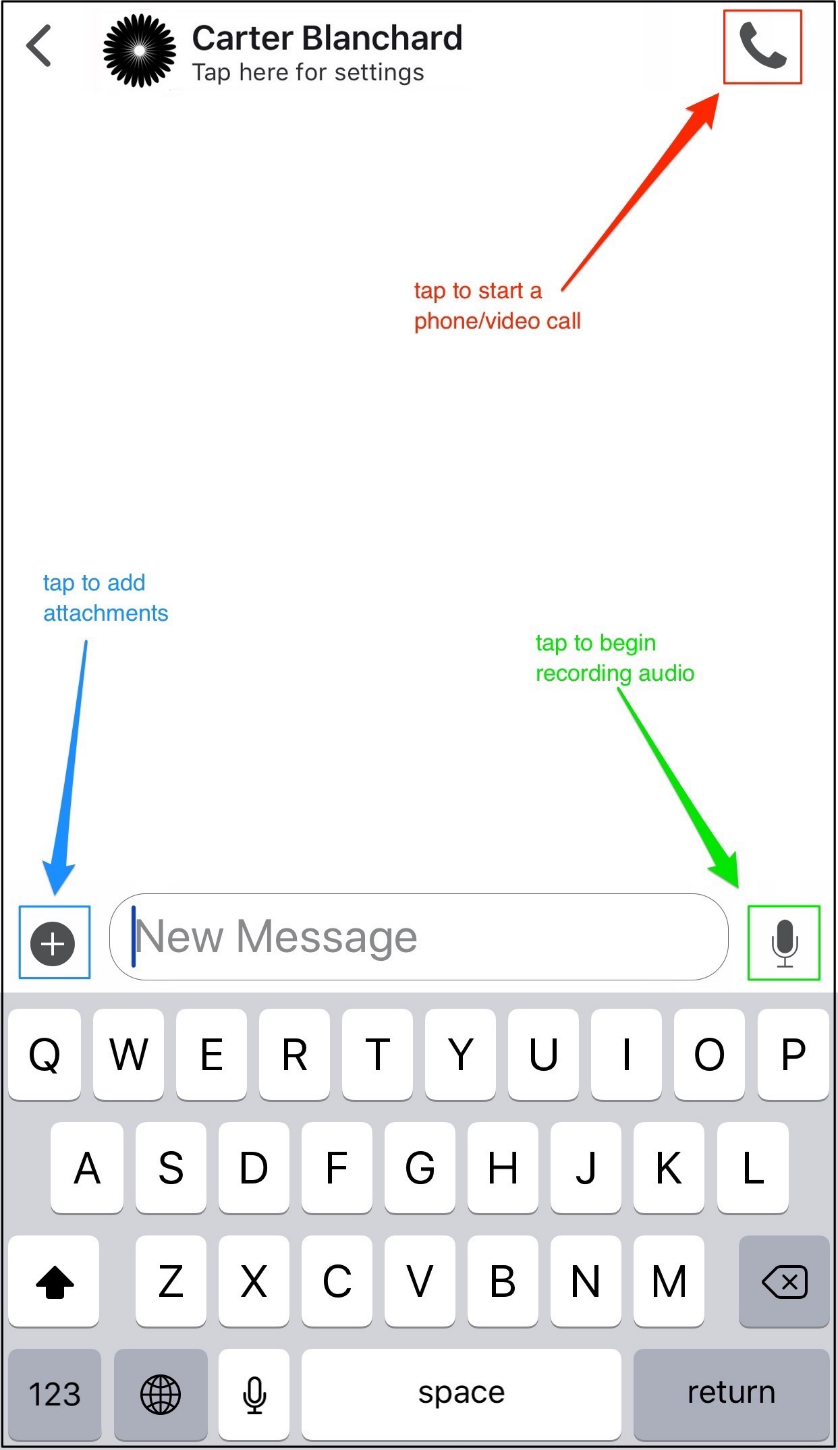
When you arrive at the main Signal application window, you’ll most likely want to press on the familiar-looking new message icon in the upper right of the active window. When you do, Signal will ask to have access to your contact list. *You don’t need to provide this if you don’t feel comfortable*: it’s only a convenience*.* Instead, you can always search to see if the people you’re trying to message are already on Signal by entering their phone numbers. That means, of course, that you’ll need to know their phone numbers. Conversely, you can choose to trust the company’s claim that they don’t store your contact’s info on their servers. At left, below, is how Signal will look (on iOS) if you’ve provided access to your contacts. At right, below, is what the app will look like if you do NOT give that access.





You can choose to provide Signal with your contact list (left) or not (right).

Once you’re set up, Signal works like most other messaging apps, so you can easily send a note, include an attachment, record audio, or initiate a phone or video call. The layout is simple and intuitive. In case you’re confused, here’s a quick infographic (on Signal’s iOS app) to help get you started:

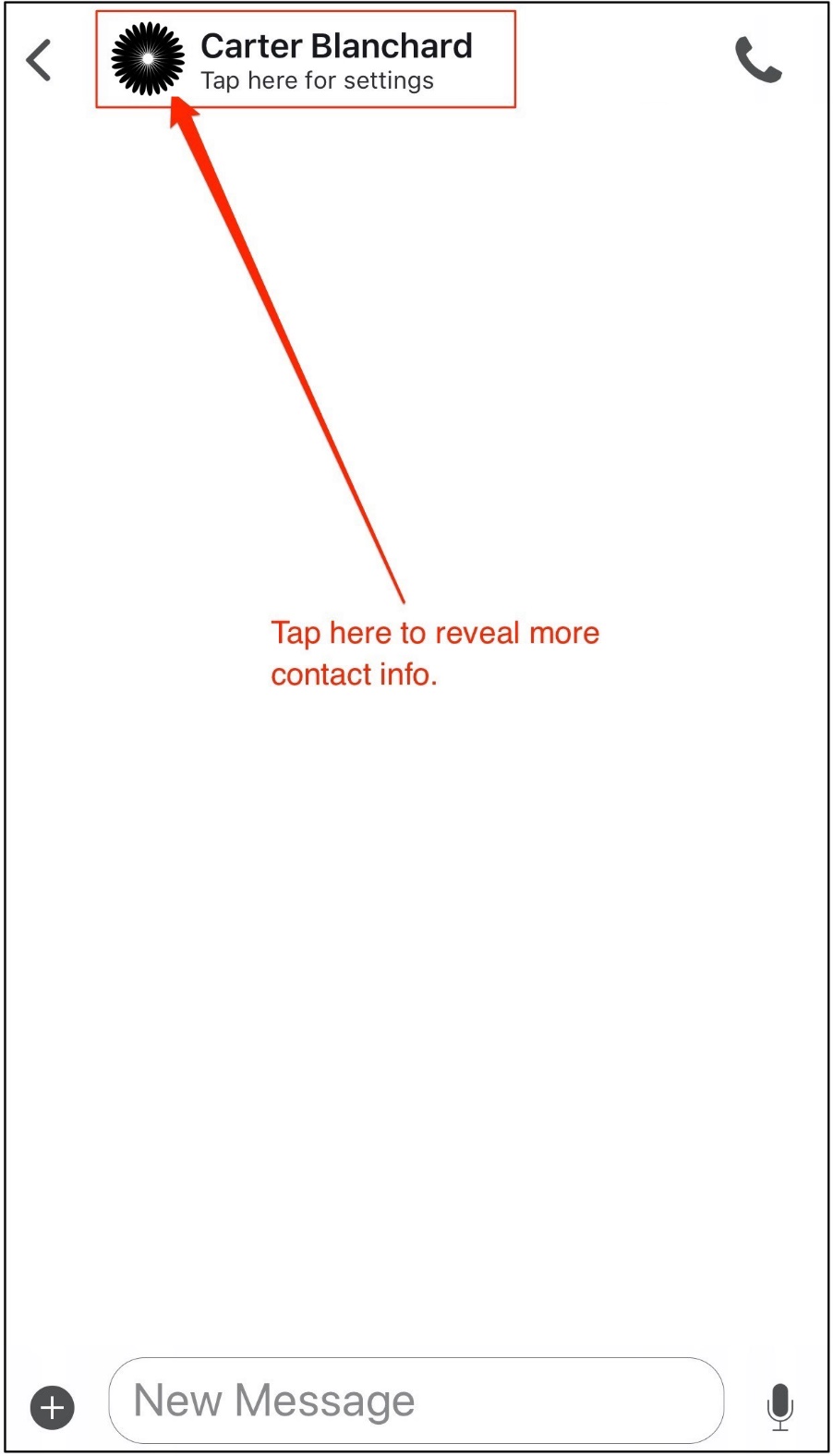


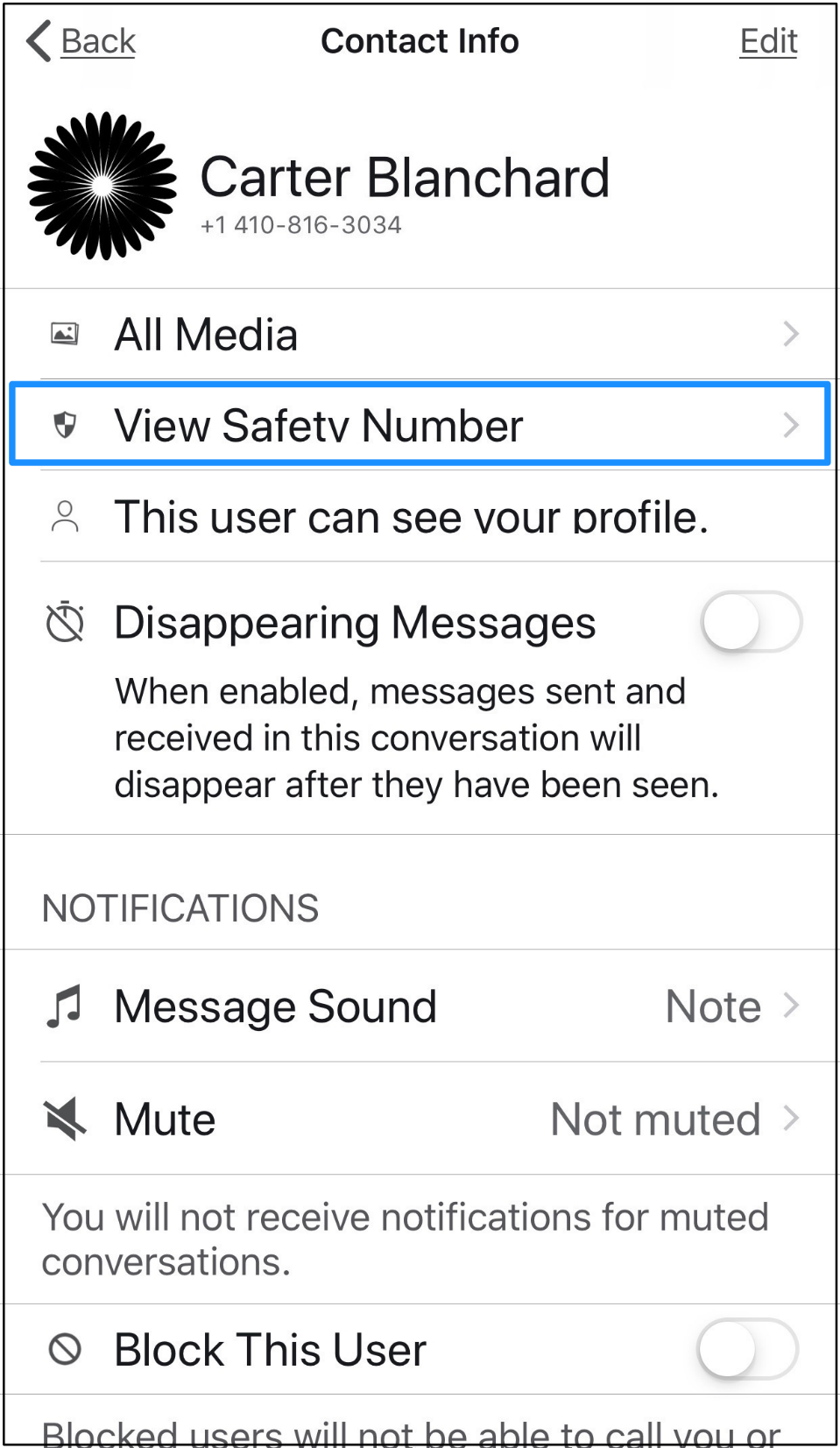
Signal has a well-stocked, easy-to-read set of [help pages for its basic functionality](https://support.signal.org/hc/en-us/categories/360000674771-Getting-Started), so while you spend some time learning the basics, I’ll instead focus on a few of its deeper security features that you should implement: safety numbers and disappearing messages.

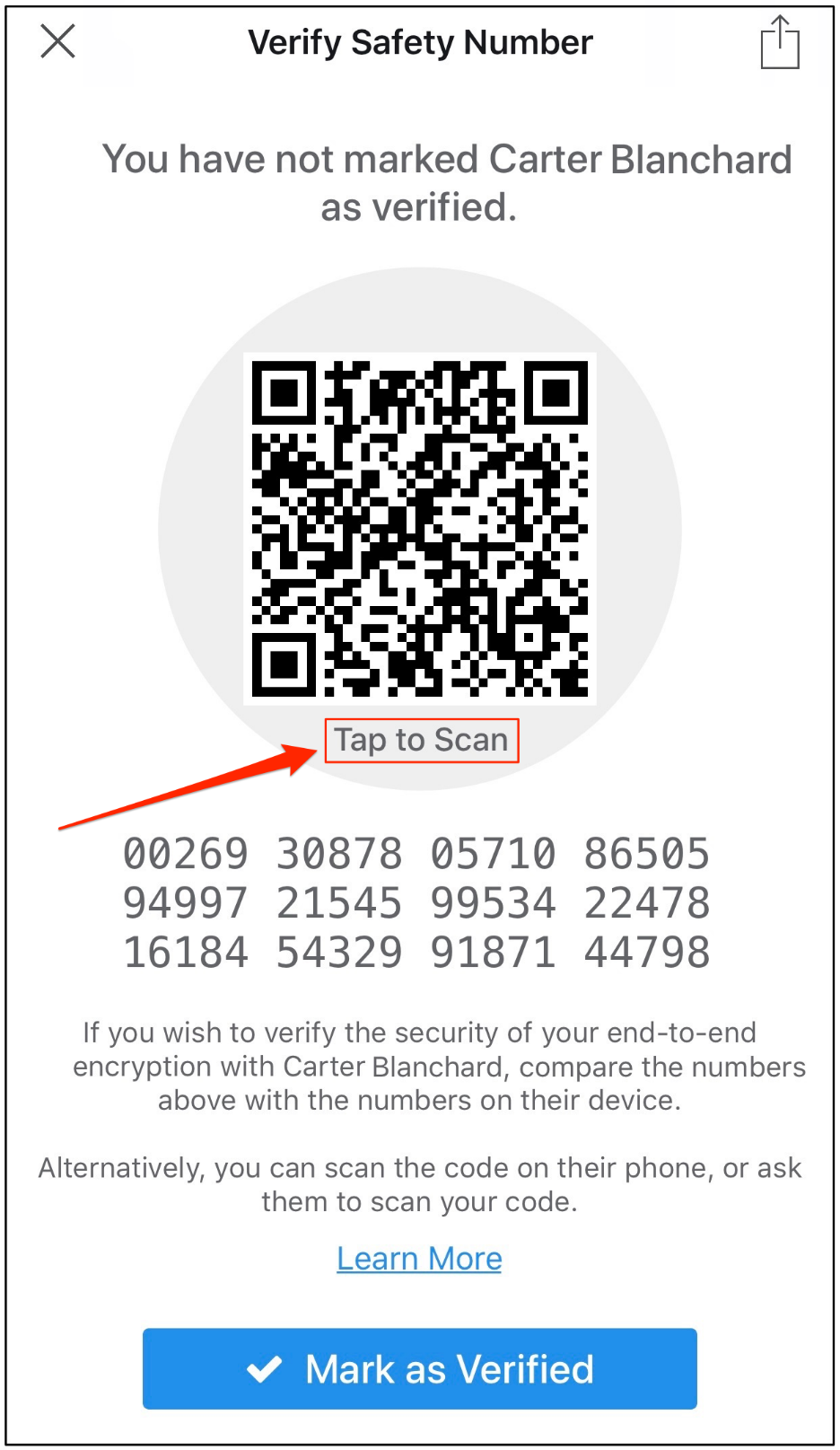
Security feature #1: Safety Numbers

[*Click here*](https://support.signal.org/hc/en-us/articles/360007060632-What-is-a-safety-number-and-why-do-I-see-that-it-changed-#safety_number_view)*for Signal’s documentation on Safety Numbers.*

On iOS, when I open a new message window with my lovely and fake friend Carter, I can tap on his avatar as shown below, at left. You’ll notice it says “Tap here for settings”. When I do this, I’m shown a variety of settings and tools that Signal makes available on a per-user basis. Let’s start by tapping on the “View Safety Number” shown center in the blue box. The contents of that screen can be seen at right.







Signal’s Safety Number feature: worth knowing about.

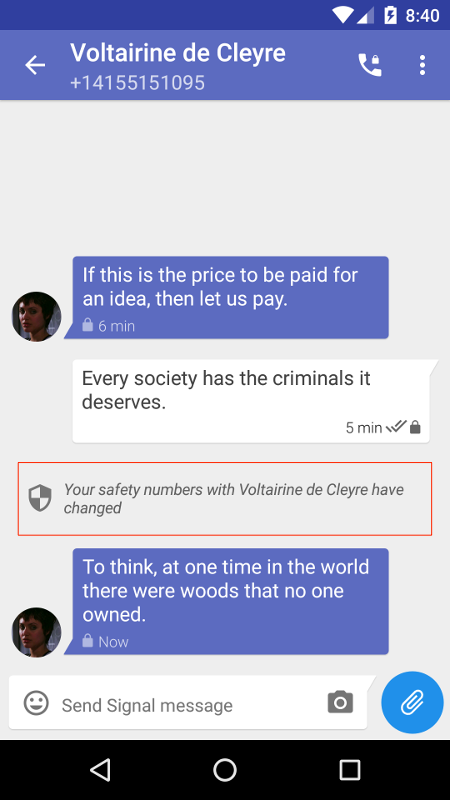


Image of Signal on Android, courtesy [Signal](https://signal.org/blog/safety-number-updates/).

The Safety Number is a Signal feature that allows you and your communication partners to confirm that your conversation with each other is secure. For those with extreme privacy/security needs, take the time to open this setting and confirm — with your intended recipient — that your numbers match. Alternately, you can choose to scan one another’s square QR code by pressing the “Tap to Scan” button as shown and verify one another in person.

[The Intercept has an excellent article on this feature](https://theintercept.com/2016/07/02/security-tips-every-signal-user-should-know/#verify) and why it’s essential.

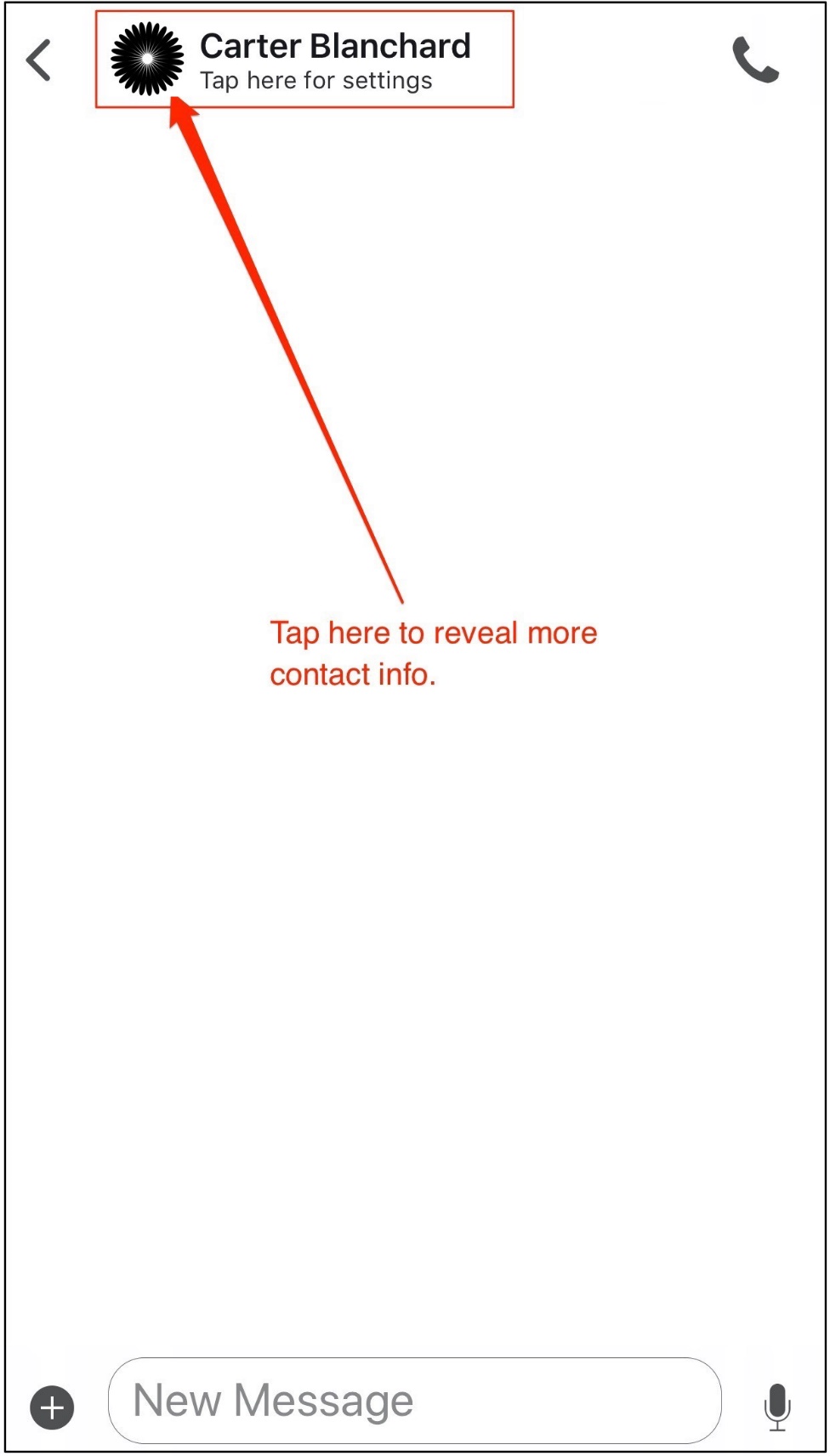
Later, if your communication partner gets a new phone and has to re-install Signal, *you’ll be warned on-screen that your safety numbers with this individual have changed*. This doesn’t mean that you’re no longer communicating with the same individual. But it might, so it’s worth confirming that fact with whatever other secure methods you and your partner have at your disposal.

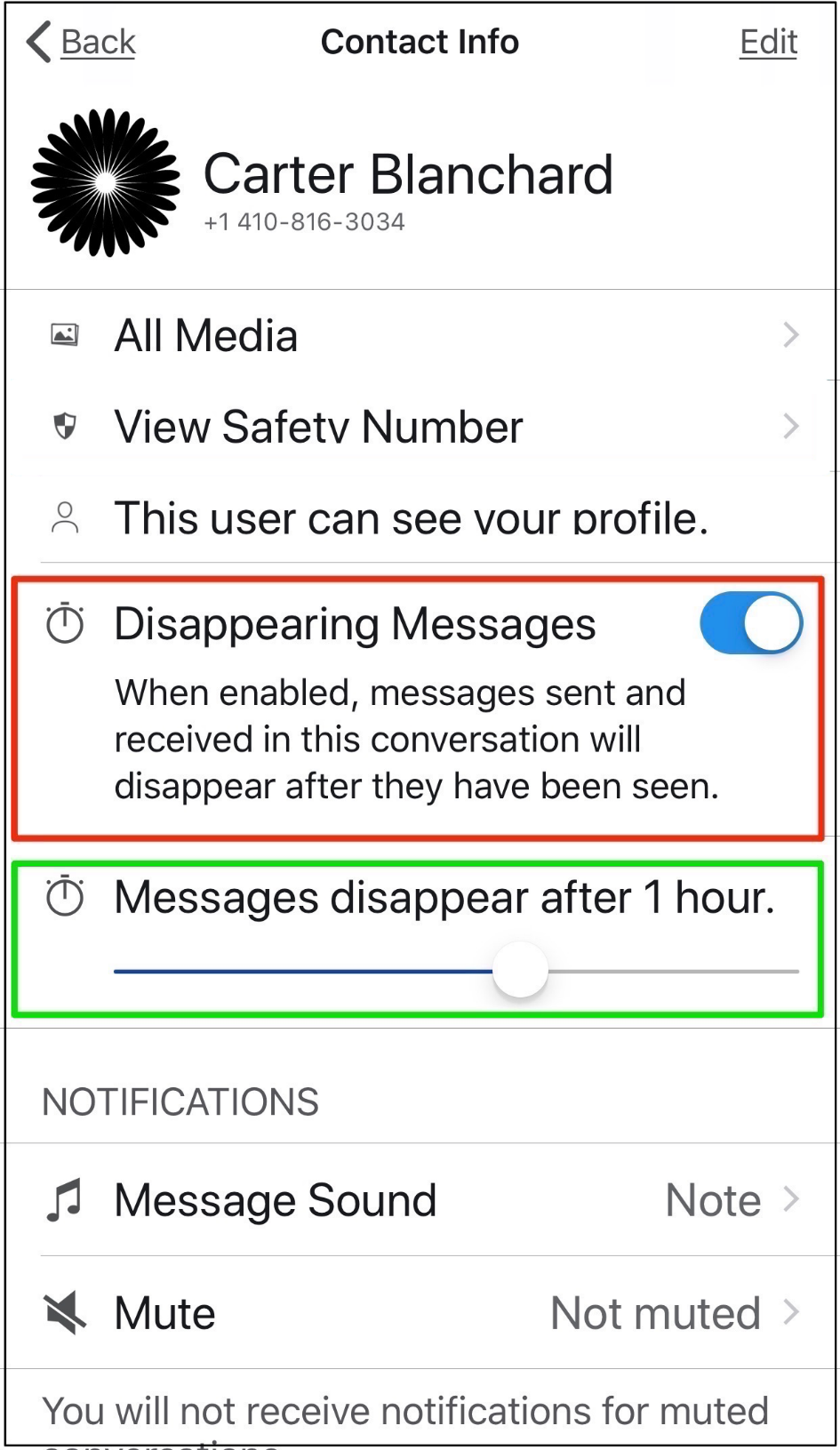
Security Feature #2: Disappearing messages

[*Click here*](https://support.signal.org/hc/en-us/articles/360007320771-Set-and-manage-disappearing-messages#ios_disappearing)*for Signal’s instructions for activating disappearing messages on iOS.*

Signal also features [disappearing messages](https://support.signal.org/hc/en-us/articles/360007320771-Set-and-manage-disappearing-messages), a tool which can help reduce or eliminate your secured conversations from being captured. Disappearing messages are activated on a per-user basis and can be set to expire from five seconds to one week. For those matters which are “top-secret”, consider a shorter period of time; for those which are “moderately-secret”, consider a slightly longer time. Use your best judgment and, whenever possible, agree to your guidelines in advance with those to whom you’re communicating.

On iOS, access to disappearing messages is activated on a per-user basis, in the same settings menu where you’ll find your Safety Number as shown here:

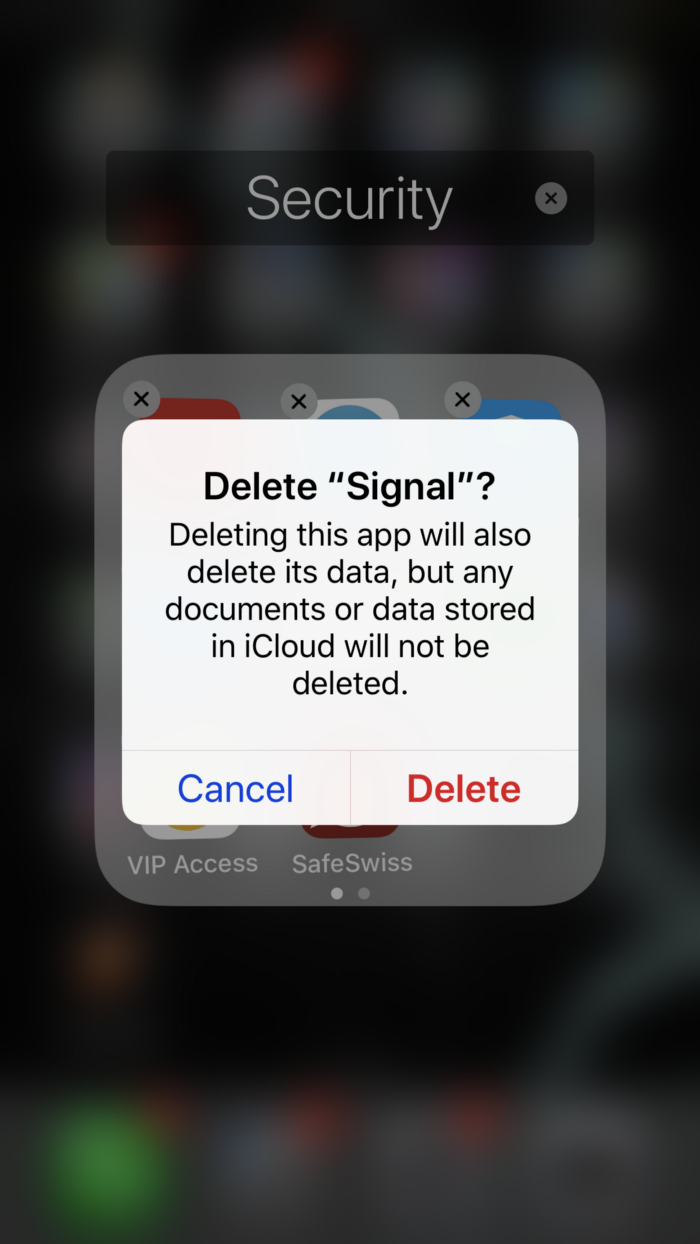




Caveats

Signal isn’t perfect, but no app, platform, or technology is. Here are a few things to consider for those of you who will choose to use Signal.

* **Don’t provide your actual cell number to Signal.** Signal only requires that you provide *some* phone number to use its service, *not your phone number*. Get yourself a valid, secondary number that’s not your actual cell phone number and provide that number to Signal instead. If you don’t know how to obtain a free, second number, read my article on [how to “classify” yourself.](https://medium.com/s/the-firewall/classified-the-art-of-restricting-personal-data-4aca5b3ffee)
* **You don’t have to give Signal access to your address book**. Signal will ask for that permission, *but it’s only a convenience.* Instead, you can always search to see if the people you’re trying to message are already on Signal by entering their phone numbers.
* **If you delete Signal, delete all of it.**If you delete the app, you’ll get this warning (on iOS). It’s a good warning: remember to delete anything that you or Signal might have stored in the cloud regarding its app.



Delete EVERYTHING, not just the app.

* **Only use the mobile versions of the Signal app.**Although Signal makes versions of its software for macOS, Windows, and Linux, don’t use it. While Signal has been good about patching (or fixing) the security holes which have occurred on [macOS](https://mashable.com/2018/05/10/signal-fixes-macos-bug/" \l "4nqIYrQTKqqG) and [on Windows & Linux](https://thehackernews.com/2018/05/signal-messenger-vulnerability.html), the truth is that your pocket computer — your cell phone — is a far better choice for security than your desktop computer anyway.
* **Only use Signal on one device.** The purpose of having secure communications is undermined if you continue to add additional devices to your Signal family. Don’t. Keep all of your secure comms on just one device: the one that you always keep in your pocket.

Runner-Ups for Secure Messaging: Wire & Threema





Wire & Threema: two excellent alternative solutions

Wire

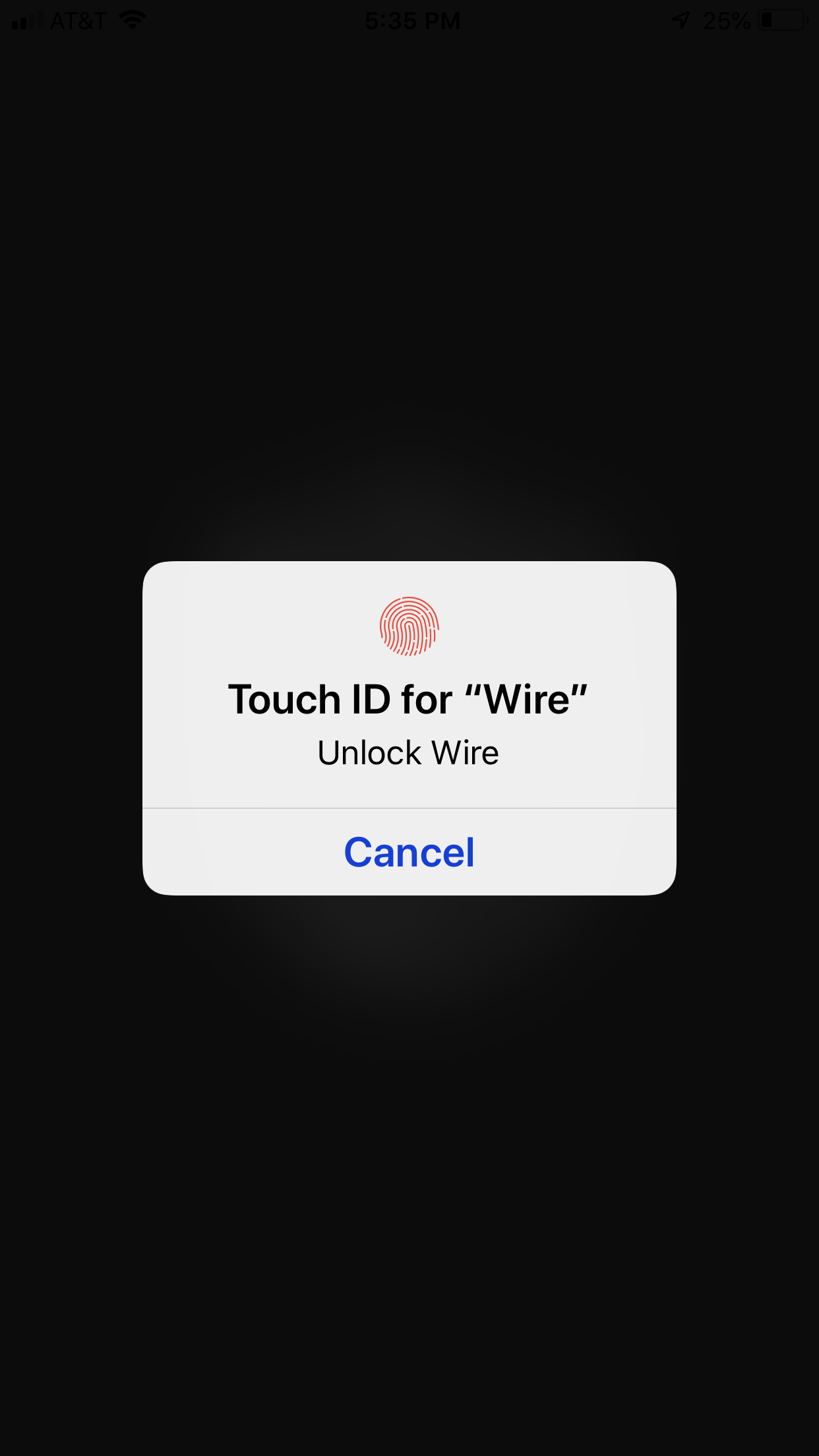
Some folks and [comparison websites](http://xn--4ca9a.eu/bac.html) rank Wire as being more secure than Signal. Others, like this fella here, just think it’s a pretty solid alternative:

I certainly understand the curiosity about Wire: it’s easy-to-use, doesn’t require you to pony up a phone number to use it, and is [regularly vetted by outside security professionals](https://wire.com/en/security/). In fact, the company prides itself on being “the most extensively publicly audited collaboration and communication software on the market” (their quote, not mine).

I like Wire because it offers something that Signal doesn’t: a security screen.

If the Wire app is open but not in use, it locks itself down from prying eyes. That means if I switch from Wire to browsing the web and then navigating back to Wire, I will NOT be able to see all of my in-progress chats. Instead, I’ll be met with a challenge — shown below — to unlock Wire using either the password it asked me to create during setup or using Touch ID/Face ID. Very smart feature. It prevents someone from grabbing my phone and having immediate access to all of my unencrypted messages.





Wire’s security screen prevents unwanted eyes from viewing your messages.

Threema

Threema offers many of the same features as Signal and Wire, but three things set it apart from the crowd:

* First, it allows you to enable two-factor authentication to better protect your account
* Second, it doesn’t require you to use a phone number to register.
* Third, it’s an app you actually need pay for.

You may wonder why I’d suggest that having to pay for an app — currently priced at $2.99 USD — is a benefit. Good tech isn’t free to build. Therefore, developers need to find funding from someone. That someone is usually another corporation. In this case, however, the public pays money directly to the developers, and that frees their parent company — Threema GmbH — from having to be beholden to any other company or government for its funding. That independence is important and 100% worth the money you’ll pay.



The safer, earlier version of email. Photo by [Samuel Zeller](https://unsplash.com/@samuelzeller?utm_source=medium&utm_medium=referral) on [Unsplash](https://unsplash.com/?utm_source=medium&utm_medium=referral).

# Secure Email

There’s one technology that we all continue to use that hasn’t evolved since the 1960s: **EMAIL.**[Email was born before the Internet](http://bit.ly/HistoryOfEmail), making it nearly fifty years old. That’s some *serious* senior citizen technology status. Despite the availability of newer messaging technology — texting, social media, Slack, and video chatting — email is not only still going strong, but it’s also actually *thriving*. In 2018, [281 billion emails were sent on average… *per day*](https://www.lifewire.com/how-many-emails-are-sent-every-day-1171210),and that’s expected to top 333 billion by 2022. 😲 👆

What’s shocking about email is that most of us continue to depend on it as it was originally designed, which is nothing short of miraculous. However, it’s also highly questionable because ***email is neither safe nor private when it comes to communicating sensitive matters*.**

Email creates—and then leaves behind—a very recognizable digital breadcrumb trail that can lead back to you. For this reason — even if you’re using a secure email solution — *you should always assume that your subject line, your IP address, the time/date stamp of your email and your actual email address can be seen by those seeking to digitally police you.* These data are known as metadata: it’s the data which reveals information about you and about your communication but isn’t the actual communication in question.

“As an analyst, I’d prefer to be looking at metadata rather than content because it’s quicker and it’s easier and it doesn’t lie.” — Edward Snowden

Given that, is there really such a thing as “secure email”?

I think there is, but it takes a bit more effort and isn’t more secure than what Signal offers.

In order to be considered secure (or “more secure”), an email service must demonstrate — at the very least — that it:

* encrypts both your messages *and* your attachments.
* allows or enables the use of PGP, also known as “Pretty Good Privacy”
* employs end-to-end encryption by default
* is independently funded or customer-funded
* has been audited by a respected third party company
* never collects customer data
* uses servers which are NOT located in the US or in any country which is a member of the [5, 19, or 14 eyes agreement](https://en.wikipedia.org/wiki/UKUSA_Agreement#9_Eyes,_14_Eyes,_and_other_%22third_parties%22)
* allows two or more factors of authentication

BONUS if the software is 100% open source and offers self-destructing messages.

After reviewing the list above and comparing those needs against [a comparison of all messaging services on the market](https://thatoneprivacysite.net/email-comparison-chart/) — sometimes [twice](https://theprivacyguide.org/tutorials/email-client-privacy-comparison.html) — there are only three top choices. [ProtonMail](https://protonmail.com/) is largely considered the best, while [EasyCrypt.co](https://easycrypt.co/) offers an interesting alternative.



Hello, ProtonMail…

## ProtonMail

There are many good reasons why [ProtonMail](https://protonmail.com/) is ranked as one of the world’s most secure email providers. It’s simple enough that anyone can use it; the platform was designed by scientists from CERN and MIT; their servers are located in Switzerland in a secure vault that’s buried one kilometer under rock (you can’t make this stuff up); they’ve been audited by [third-party security professionals](https://protonmail.com/blog/openpgpjs-protonmail-security-audit/). Even better, ProtonMail offers a 100% free tier, so you have no excuse to not sign up and give it a try.

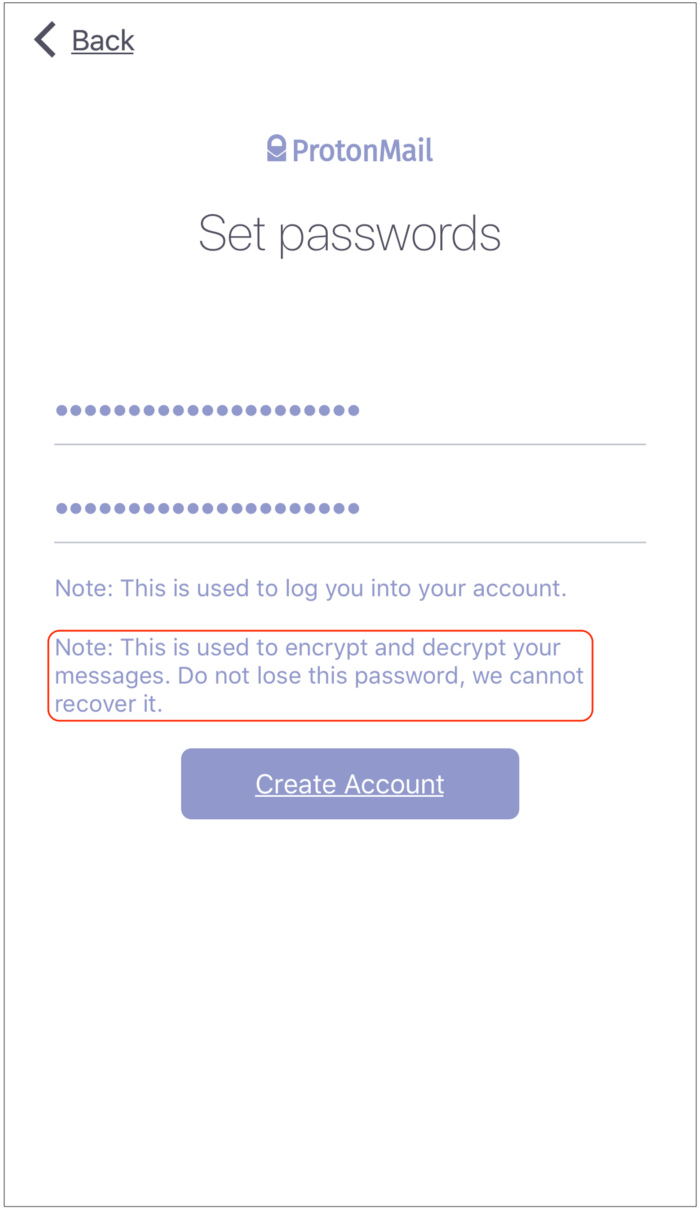
More importantly, all messages sent from one ProtonMail account to another are encrypted with PGP. PGP, or “Pretty Good Privacy” (I know, the name is hysterical) is a decades-old and extremely well-respected security protocol for sending secure and encrypted emails. What’s so great about ProtonMail’s version of PGP is that it all happens behind-the-scenes, by default, with no extra work or setup required on your part.

Therefore, one of the easiest, cheapest, and most secure ways that you and your sensitive contacts can email one another is for you all to have accounts on ProtonMail and only email each other using that system.

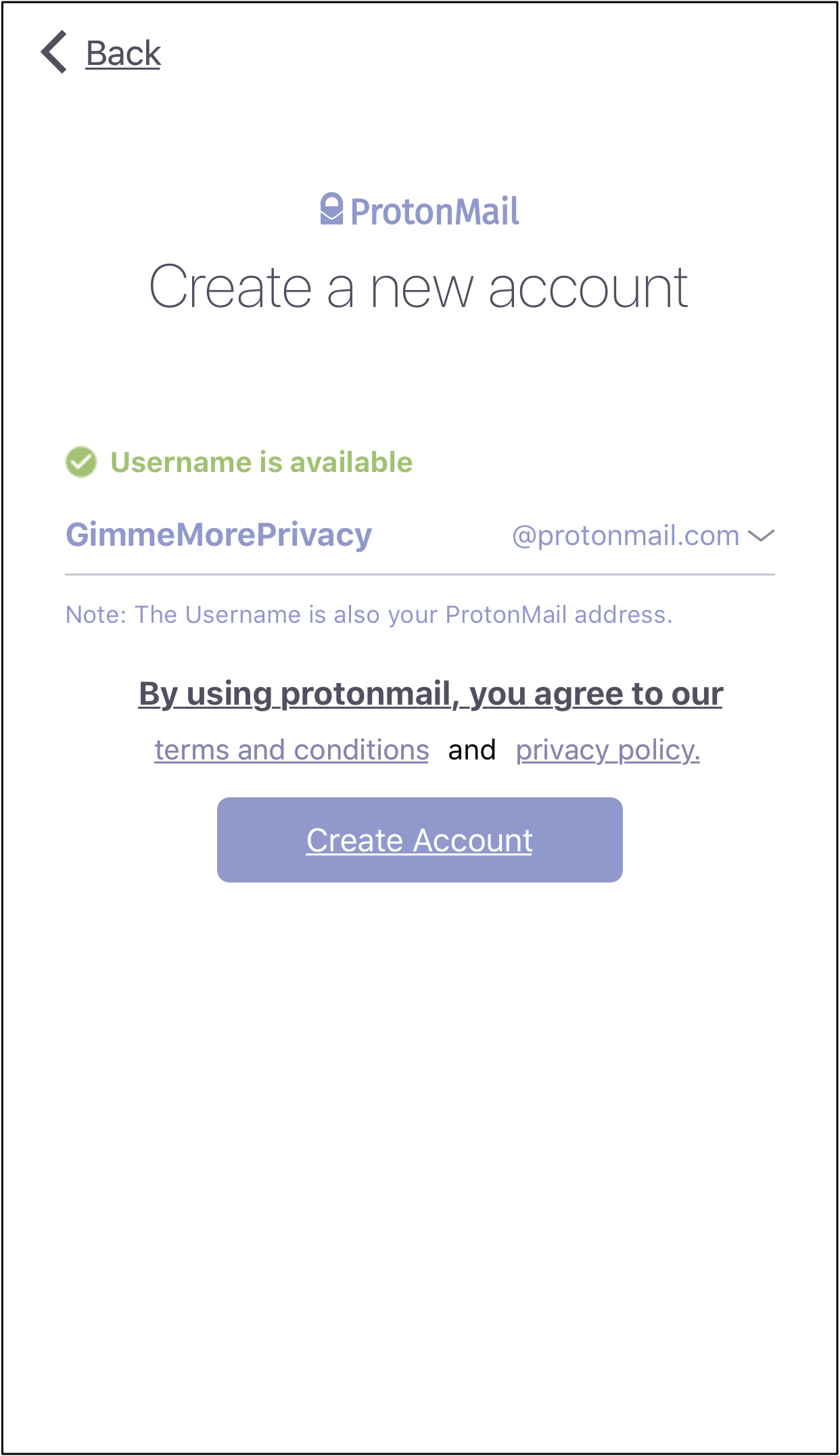
### Setting It Up

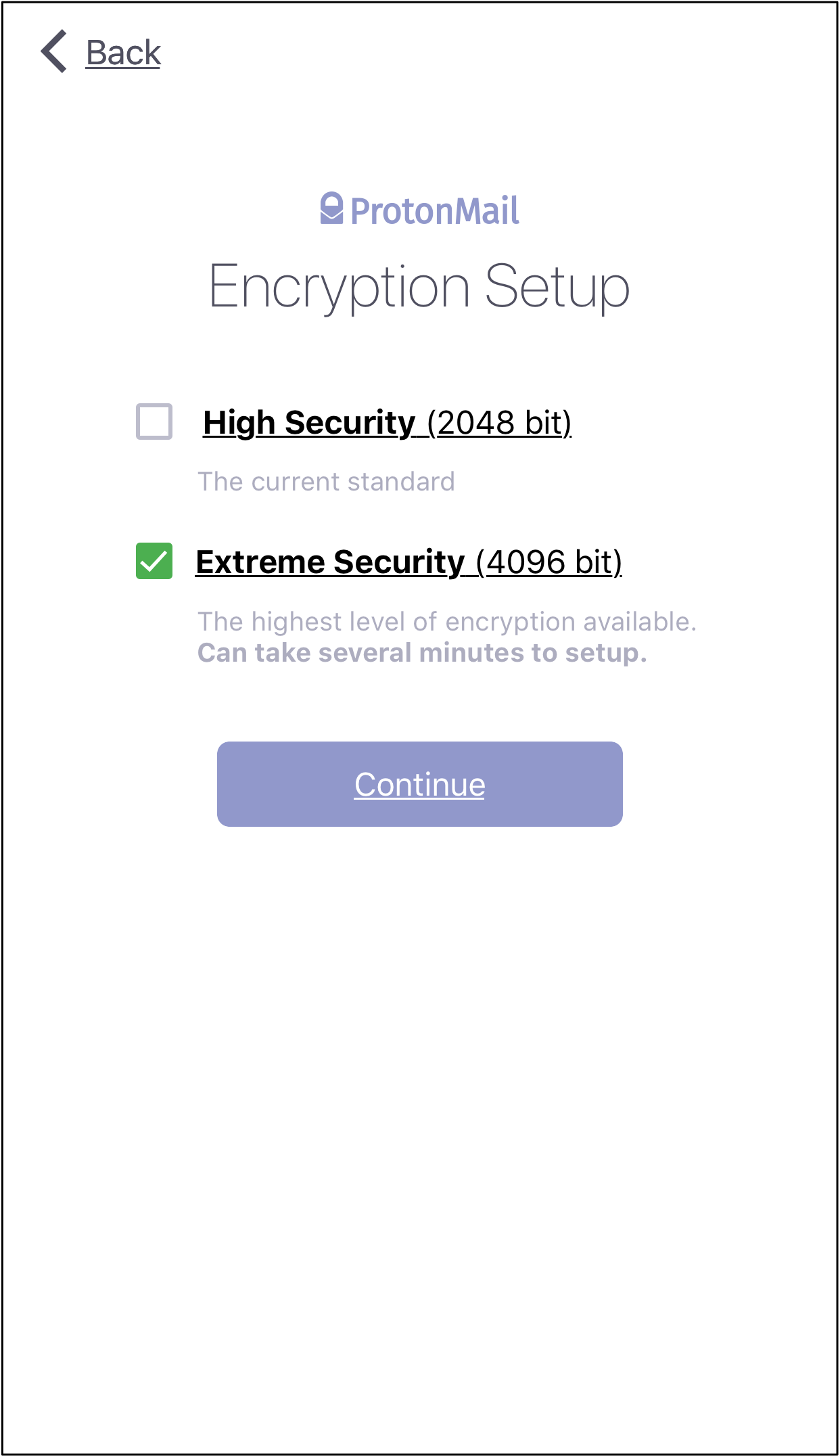
Setup is easy: simply [download the ProtonMail app](https://protonmail.com/secure-email-app) for iOS and follow the prompts to create and set up the service. You’ll be led through a series of windows to establish your account. For those with the most pressing needs, choose the “Extreme Security” option.

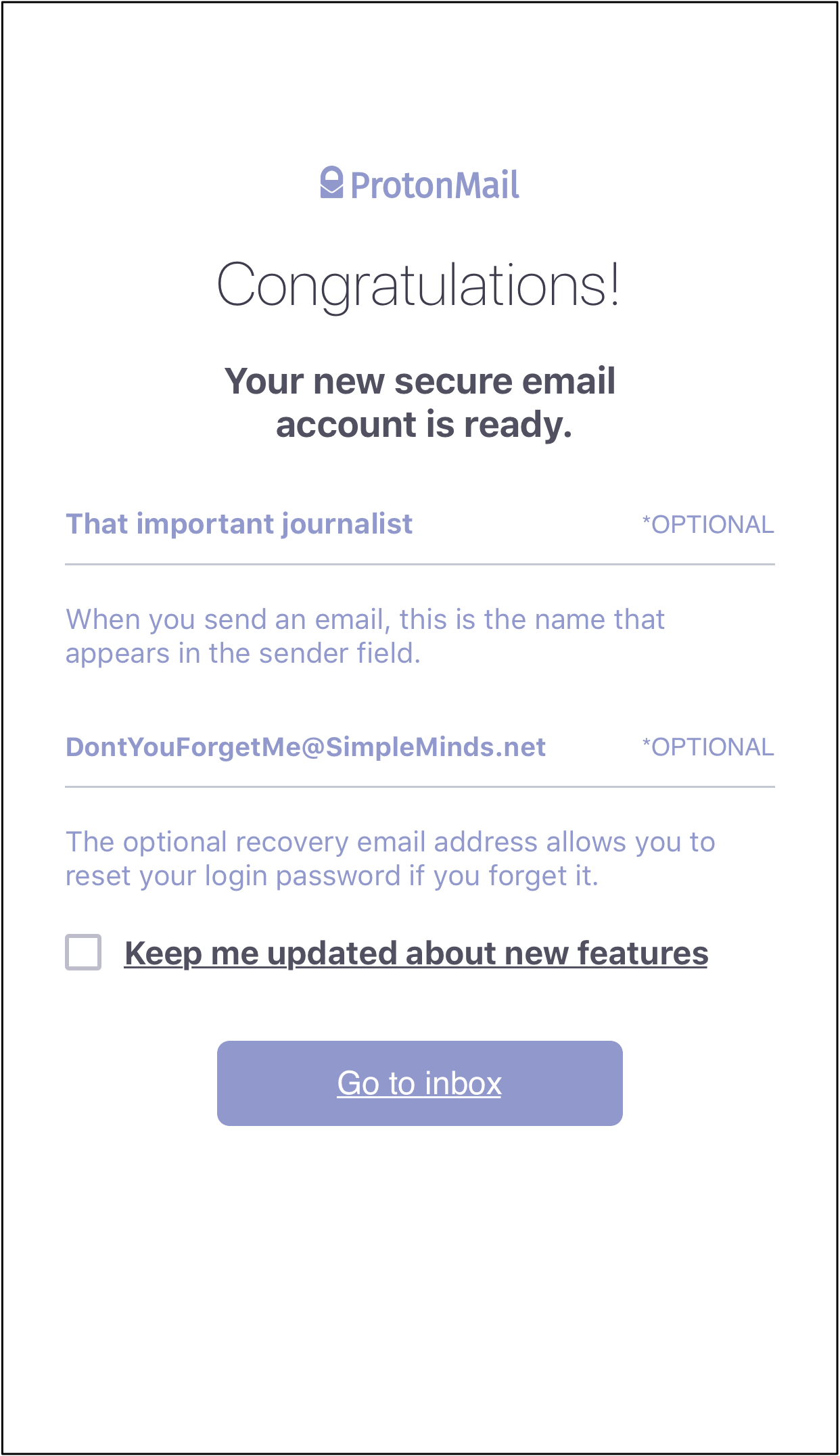
Worth noting: no phone number or email address is required to set up your account. You may elect, for convenience, to provide ProtonMail a recovery email address if you’re the kind of person who forgets your login password. If you’re a whistle-blower, informant, spy, or citizen in a brutally repressive regime, do NOT use a recovery email address. Instead, just remember your password, OK?



Do. NOT. Lose. Your. Password.



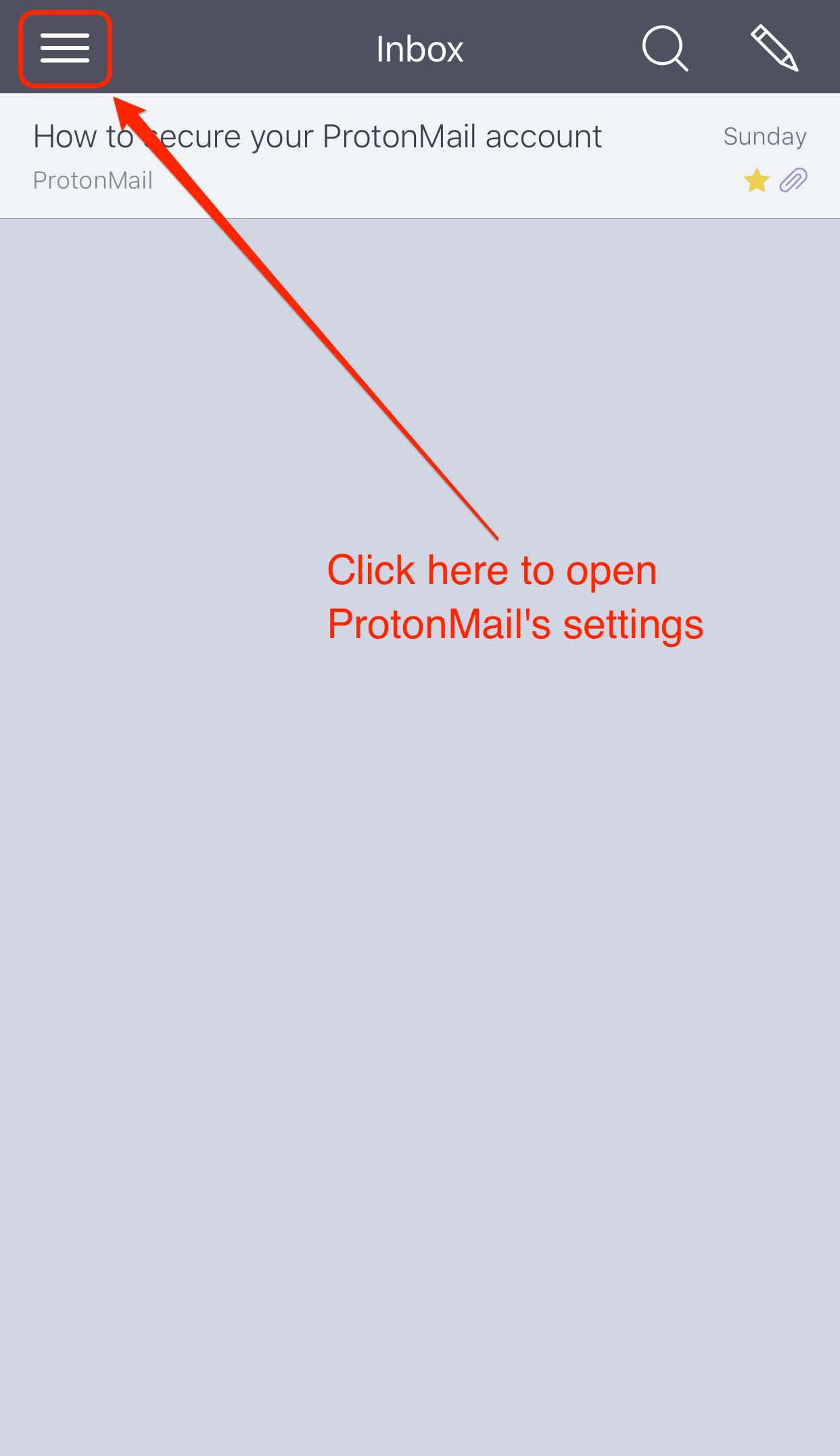


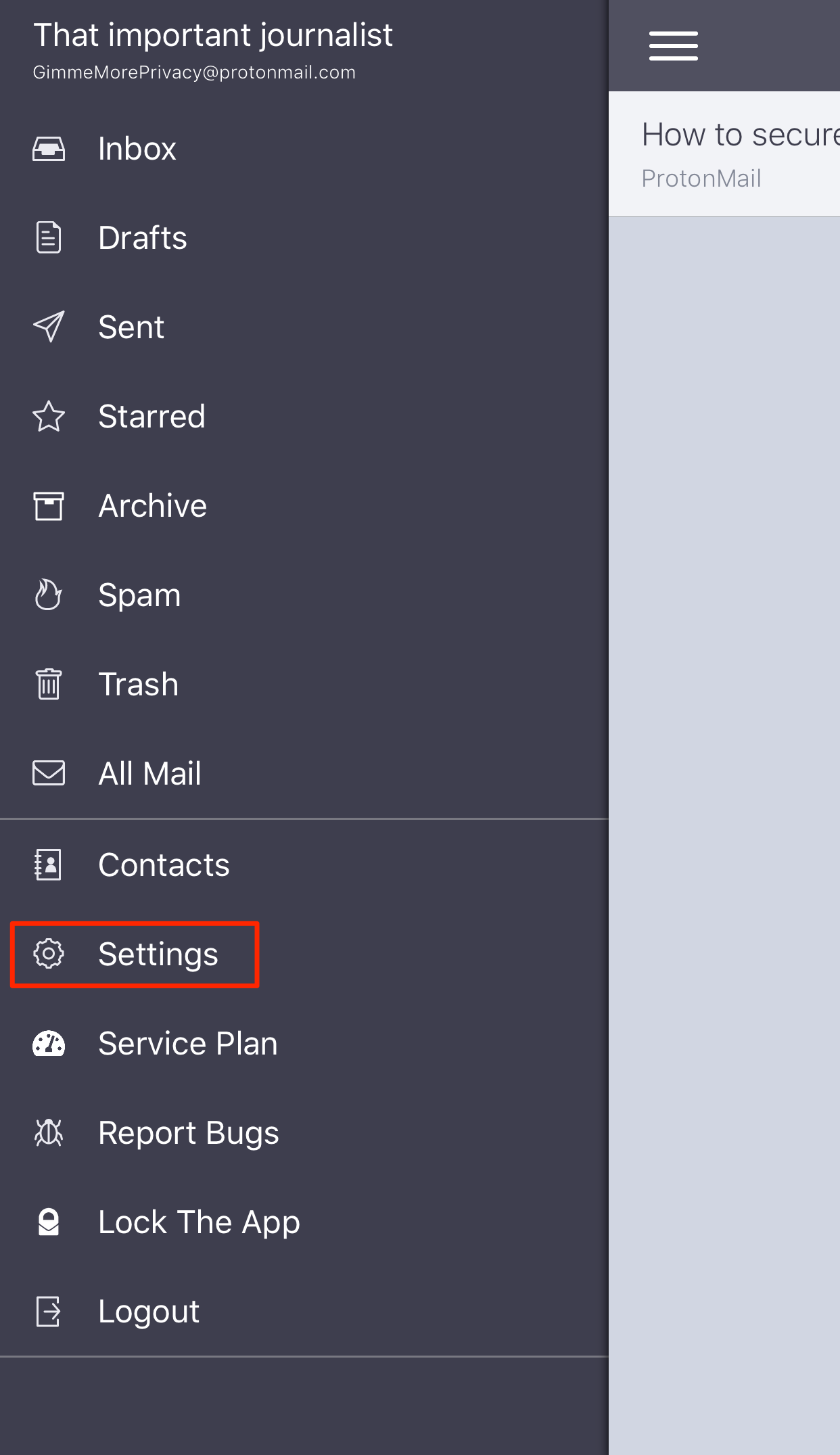


Some of ProtonMail’s setup windows.

### Using ProtonMail

Once you’ve logged in, ProtonMail is just as easy to navigate and use as any other webmail service. Know how to use Gmail or Outlook? Then you’ll intuitively already know how to use ProtonMail. There’s a recognizable navigation button in the upper left of the application window. Touching that allows you to navigate your ProtonMail account folders, along with the application’s full suite of preferences.





Navigating ProtonMail’s folders and settings is a breeze.

You’ll notice that I’ve highlighted the “Settings” control. That’s because the very first thing you need to do is protect the ProtonMain application with a security PIN. Touch **Settings -> Enable PIN protection**. You’ll be prompted to enter a numerical password twice: once to set it, and a second time to confirm it. Setting this PIN locks the ProtonMail application from view if you switch to any other application on your iPhone, including viewing the desktop.

This is similar to what the Wire secure messaging app provides by default, and it’s a simple and protective measure to take. Doing this ensures that no one can grab your phone and see the contents of your ProtonMail without also knowing your PIN. This step is so important, I’ve created a video for you. For those paying attention, you’ll see that I’ve set my PIN to “8675309” so the only other person — in the entire world — who’d ever know my password is, obviously, [Jenny](https://www.youtube.com/watch?v=6WTdTwcmxyo).

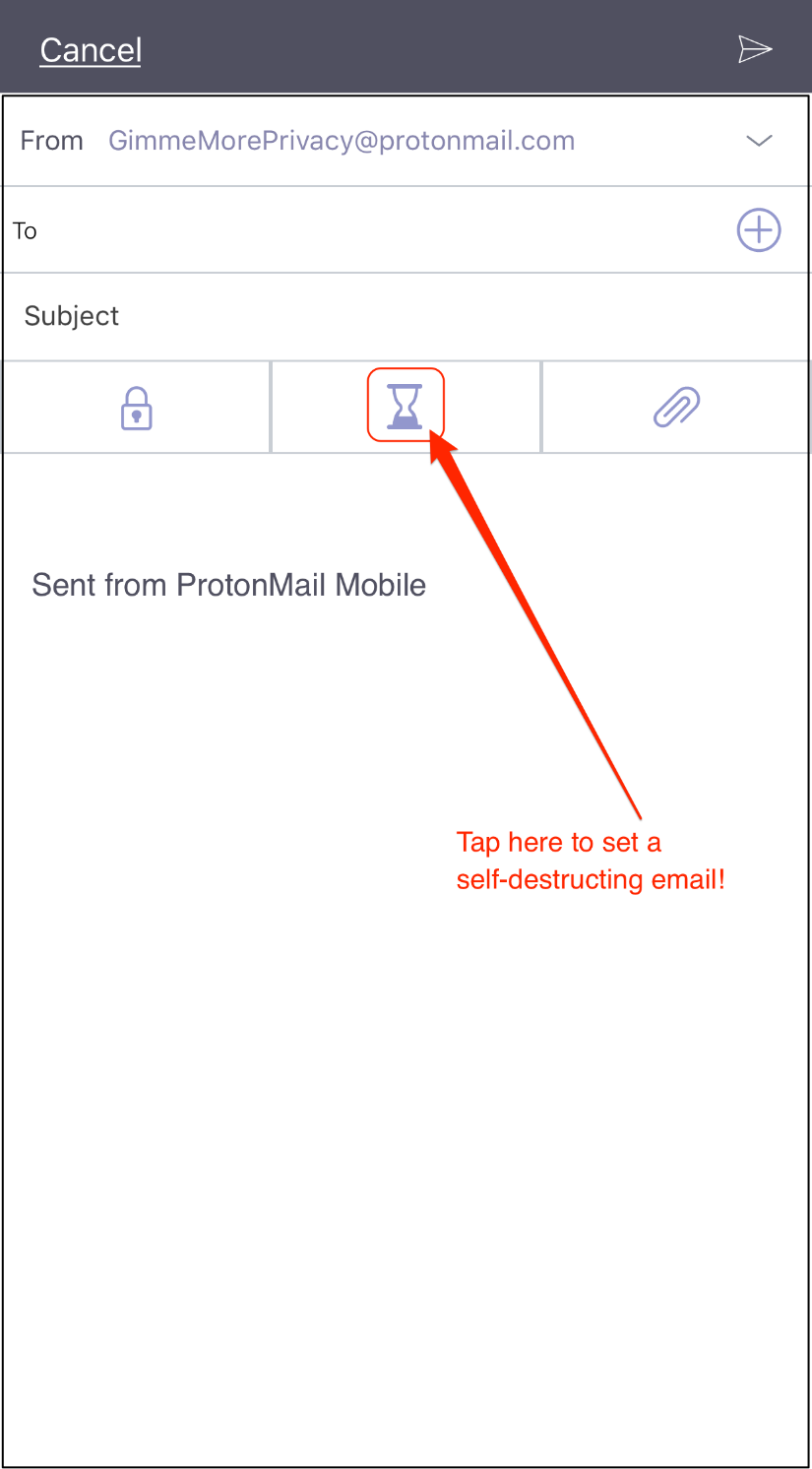
Video by the author.

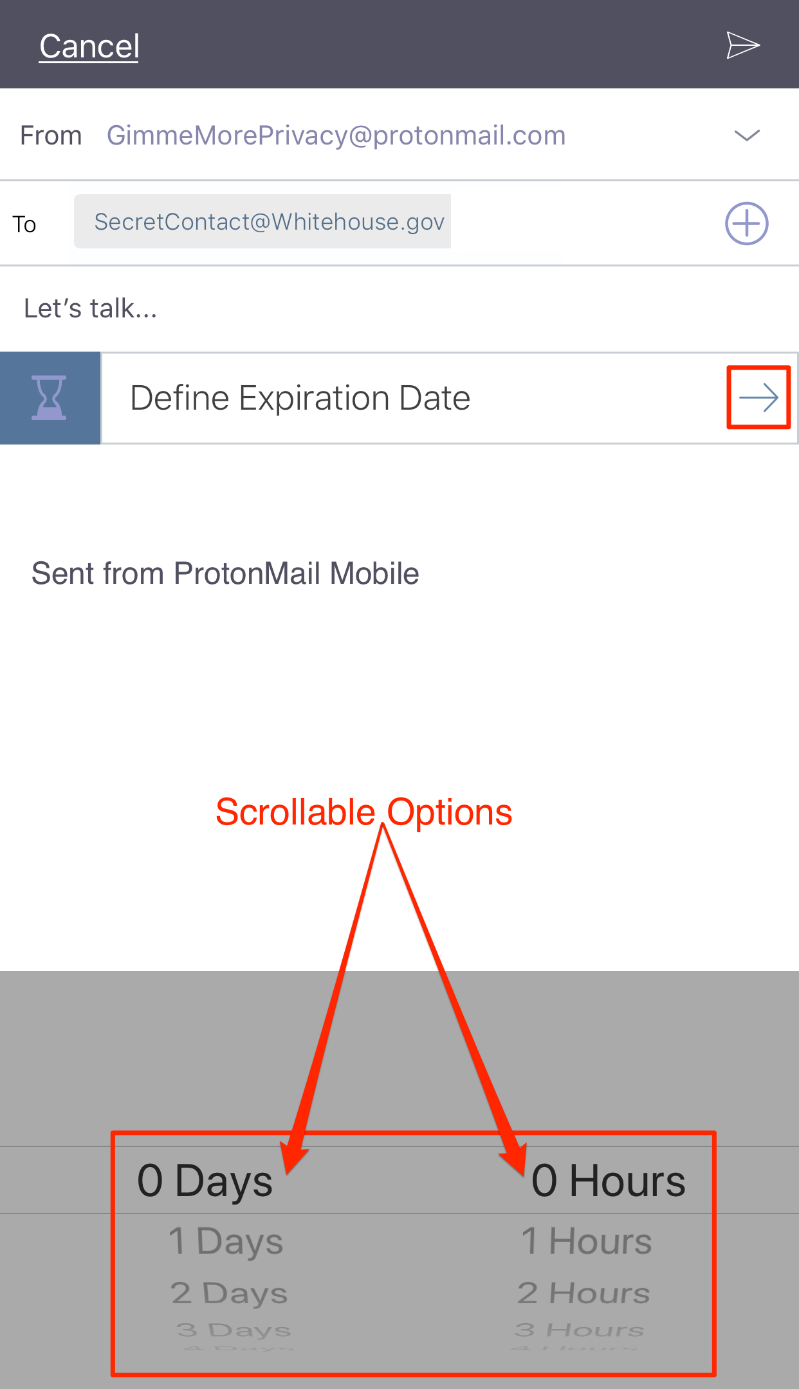
### Security Feature #1: Expiring Messages

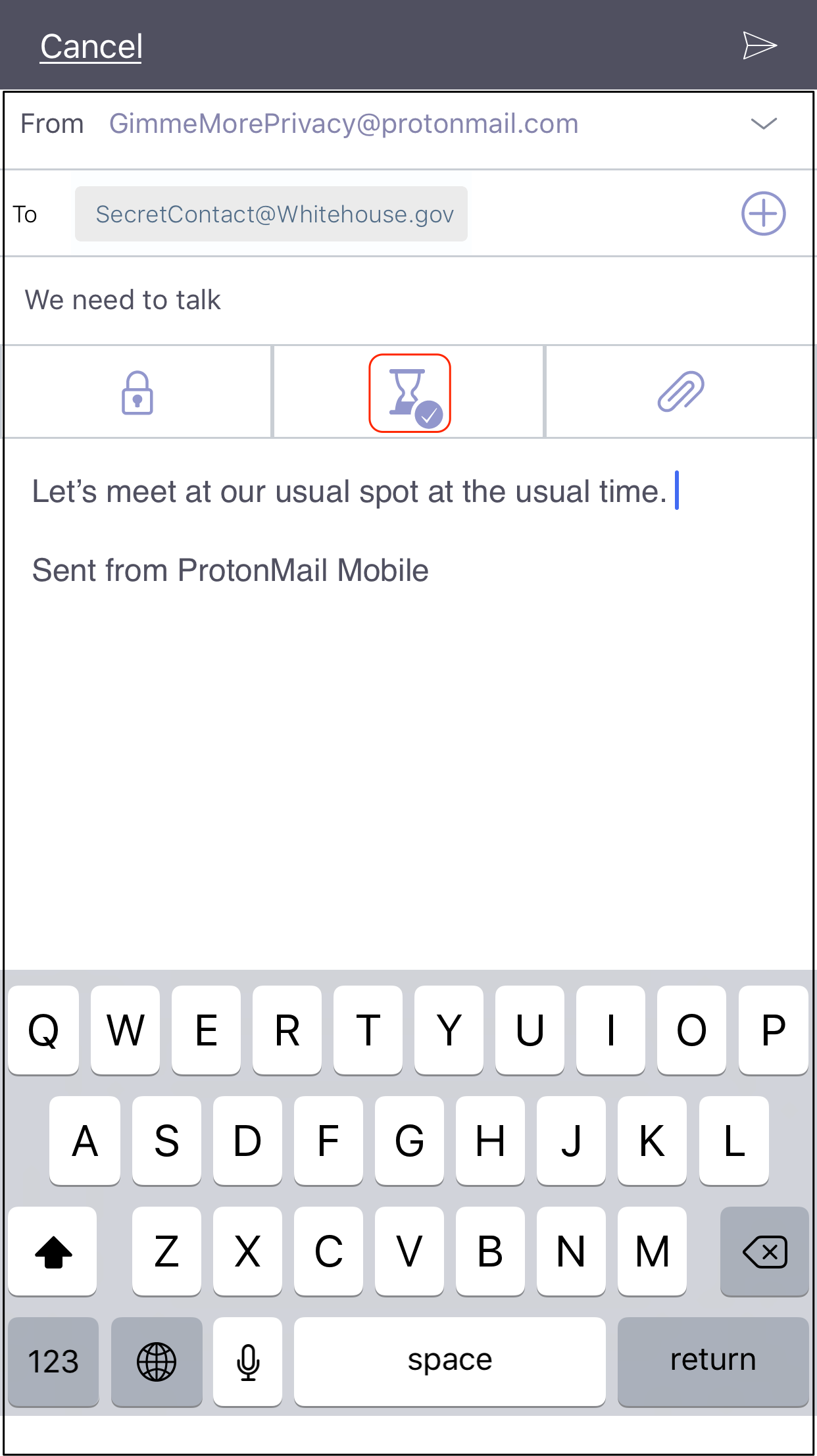
By default, ProtonMail messages don’t expire. But [ProtonMail gives you the power to set an expiration time on any email message](https://protonmail.com/support/knowledge-base/expiration/)! It’s like “Mission Impossible”: pretend you’re Agent Ethan Hunt and get yourself some self-destructing messages! If you choose to leverage this amazing tool, you can choose an expiry time between one hour and 29 days, 23 hours. For the most secure messages, choose a short time.

To access this feature, open a new message. Then, click on the hourglass icon as shown below at left. Using the two scrollable fields at the bottom of your new message, choose the number of hours and minutes before your email will disappear forever, then click the arrow as shown below, center. Once your expiration date is set, the hourglass icon will change to include a checkmark, as shown below, right. Now, you can add an email address, subject line, and the body of your email.

When you’re ready to send, click the plane icon at top right.





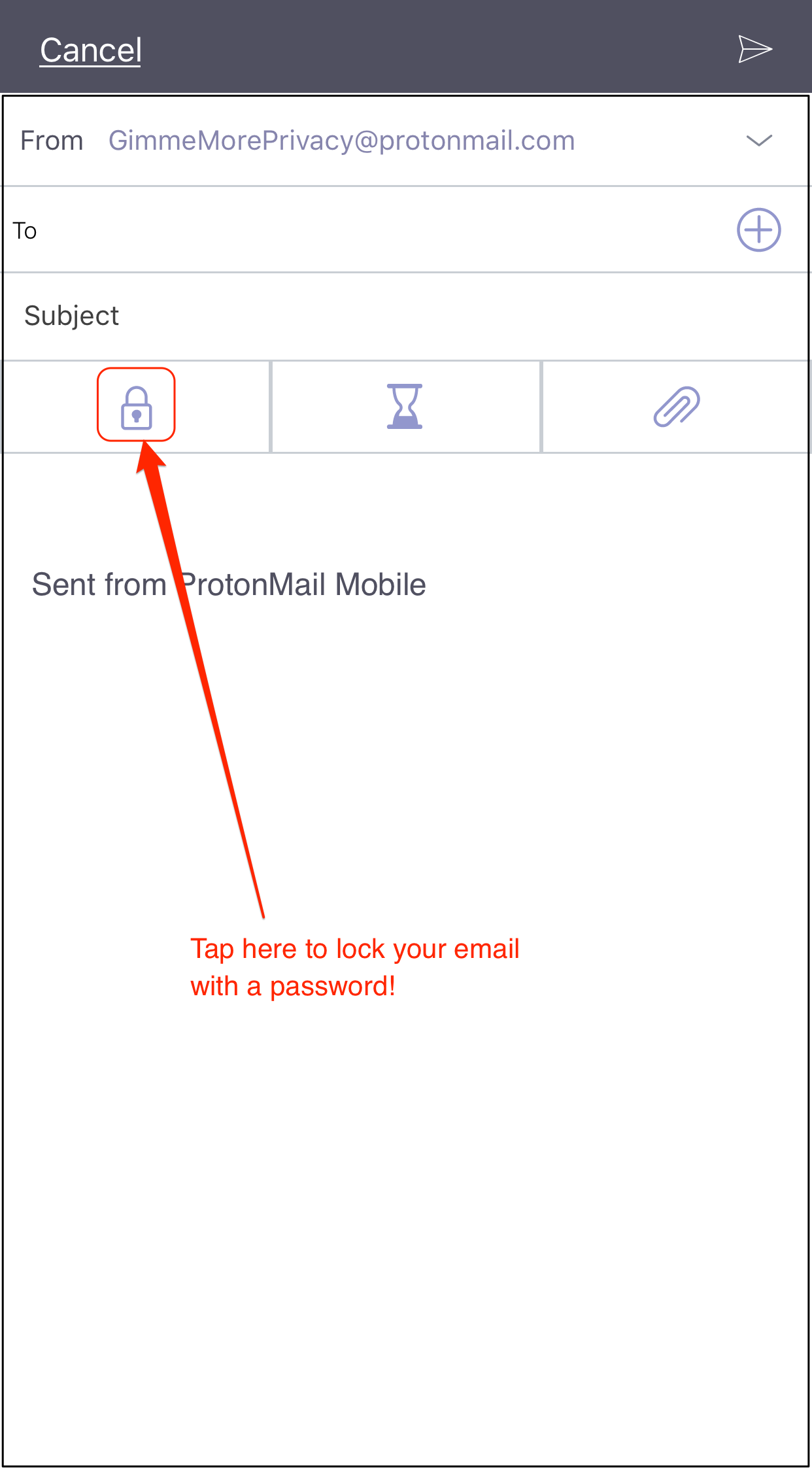


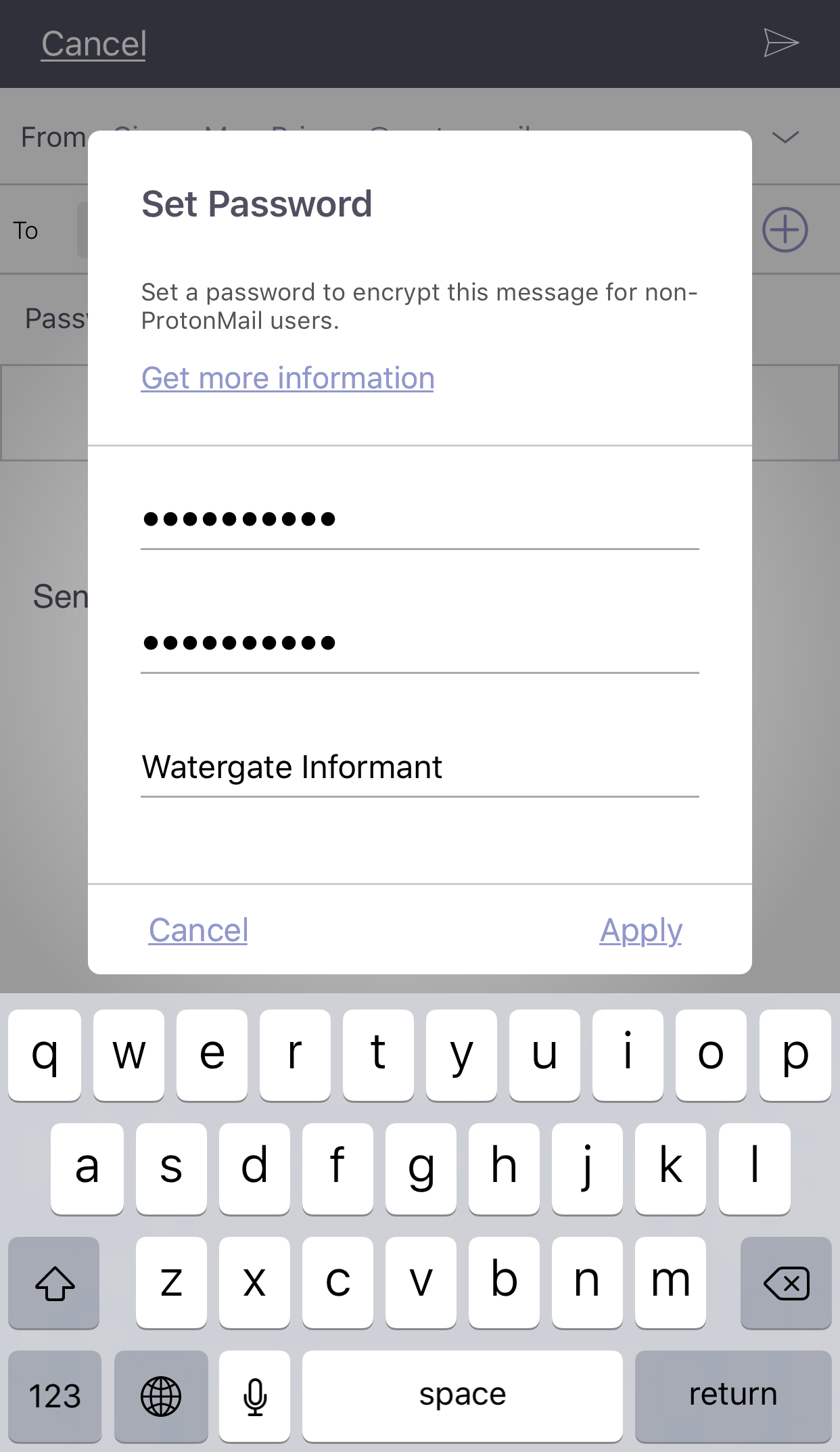
### Security Feature #2: Password Protected, Encrypted Emails

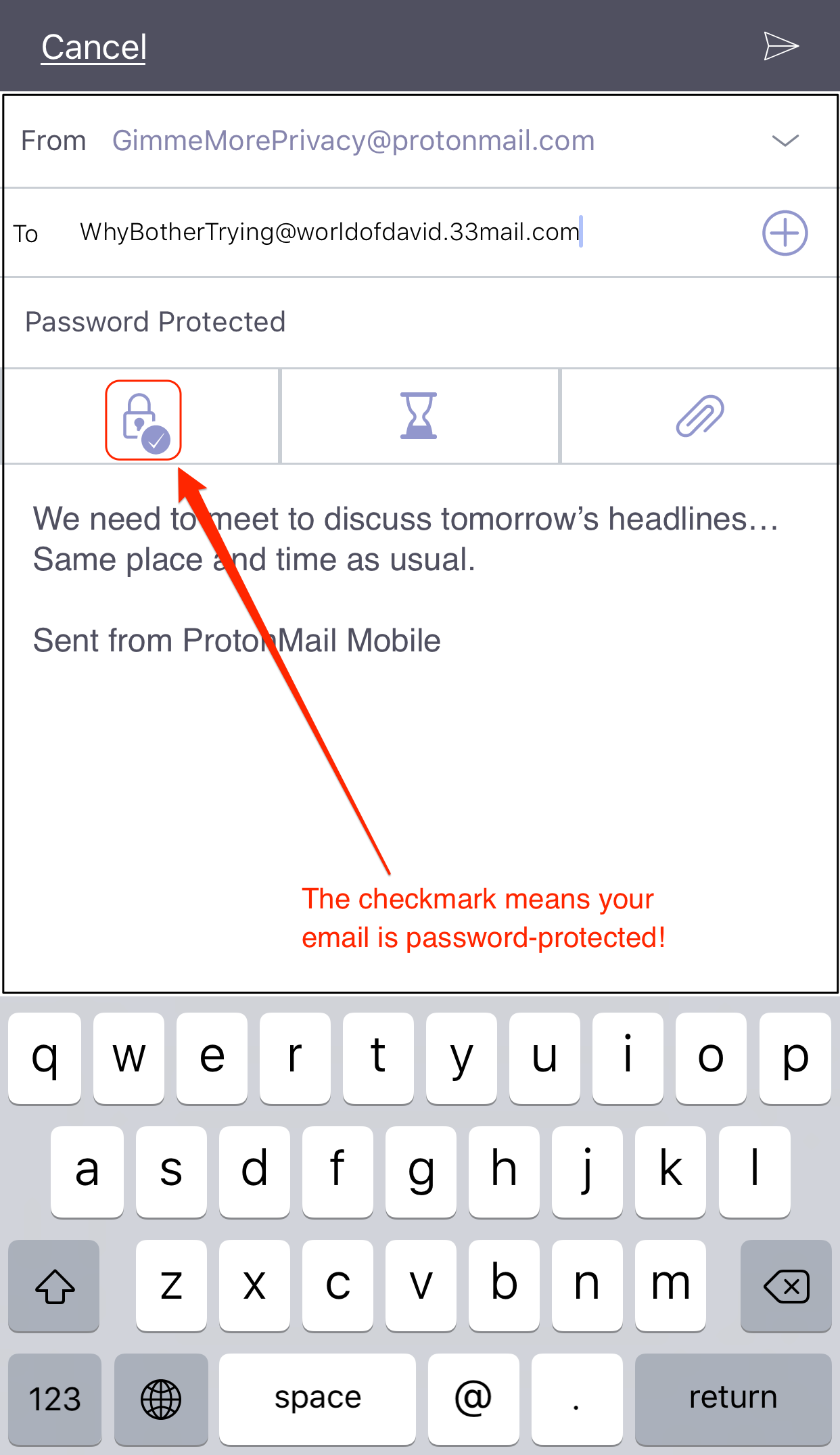
I mentioned earlier that ProtonMail, by default, enables encryption for all emails sent between all ProtonMail accounts. But what if the person you need to email is not a ProtonMail user? Good news: *[ProtonMail also allows you to encrypt messages to anyone outside the ProtonMail system.](https://protonmail.com/support/knowledge-base/encrypt-for-outside-users/)* This functionality is easy to use, incredibly smart and built right into the system.

To begin, open a new message window and click the lock icon as shown below (left). When you do, you’ll be met with a prompt (below, center) asking you to provide and then confirm an encryption/decryption password for your email. ProtonMail permits you to include a hint for that password when your notification is delivered! Before you send your email, confirm that it’s protected with a password by looking for the checkmark on the lock icon as shown below, right.

Here’s how ProtonMail makes this nifty security feature work: non-ProtonMail recipients don’t actually receive your email; instead, they receive a link to view your email on ProtonMail’s servers. That email remains encrypted to anyone who doesn’t possess the password. This is why it’s important to *only share the password with your intended contact through a method other than email:* use a phone call, text, fax, mimeograph or — if you’re extremely old school: smoke signal. Just don’t send an email password to someone using email, OK?

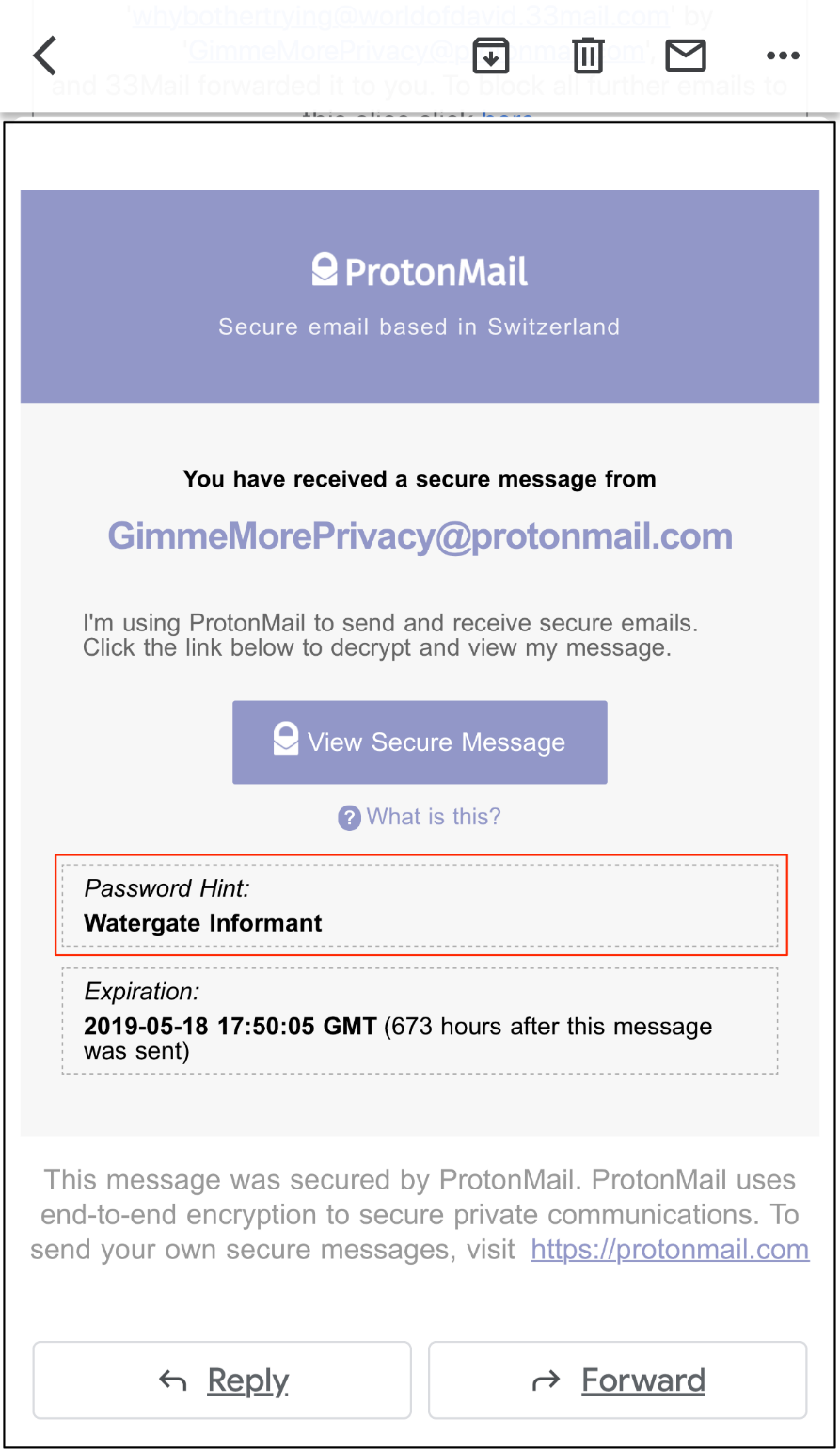


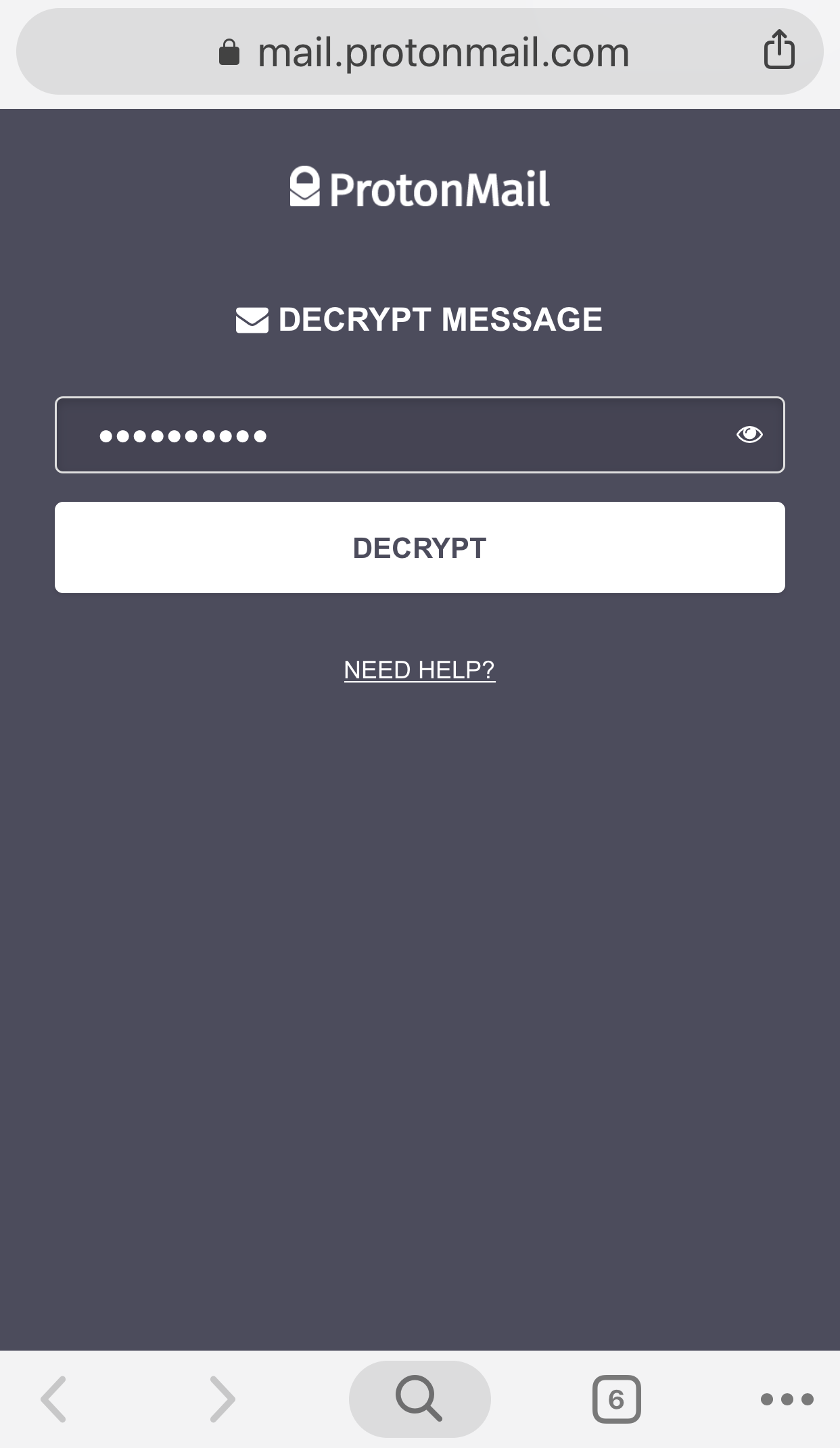


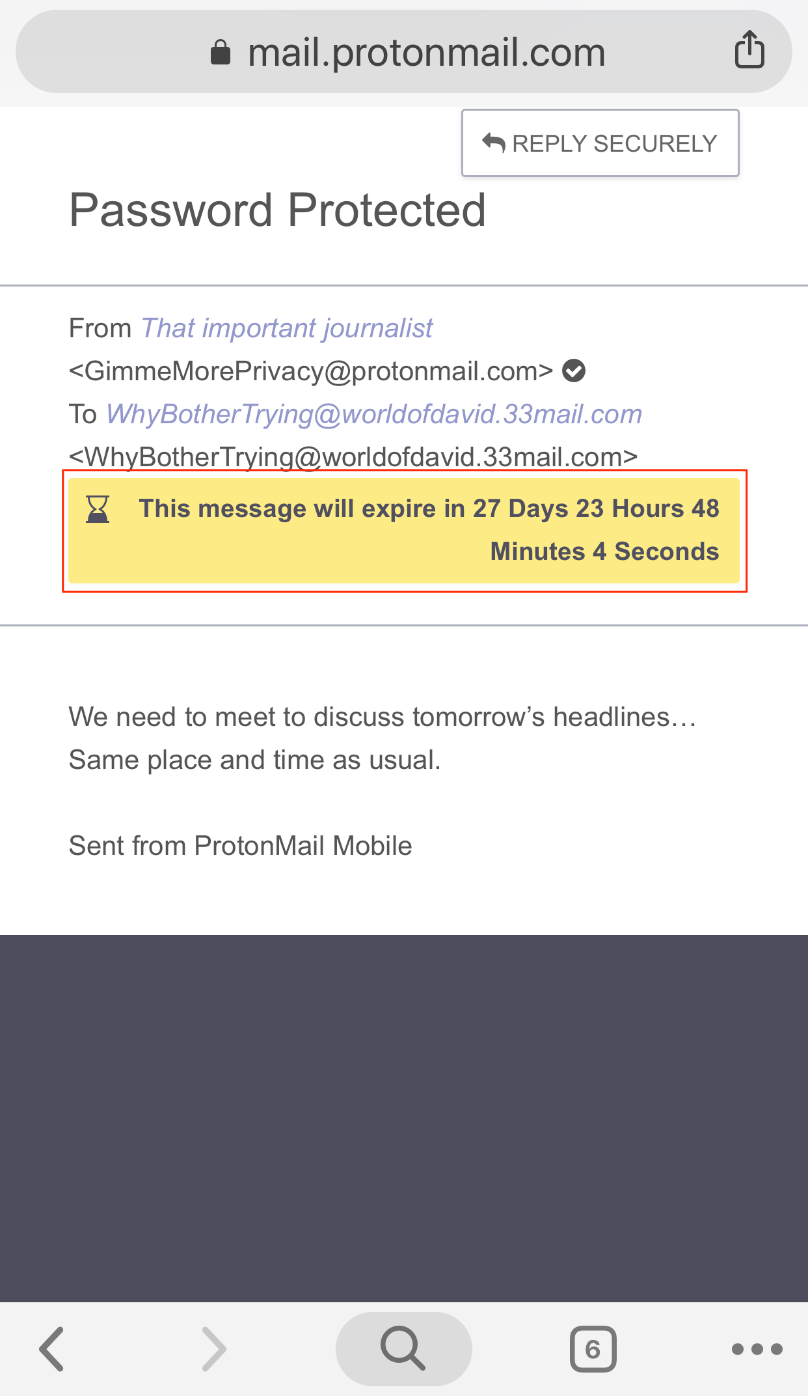


Sending a password-protected email in ProtonMail.

Receiving a password-protected email from a ProtonMail user is also worth sharing. Non-ProtonMail users receive an alert that they have a secure message. That email includes the password hint that you remembered to include as shown in the red box below (left). Clicking on the blue “View Secure Message” button opens a browser window and prompts the user to enter the decryption password below (center). Once the correct password has been entered, your email is displayed as shown below (right). Note that all secure messages, by default, time out after 28 days, as shown in the yellow box.







Receiving a secure message from a ProtonMail user.

### Caveats

ProtonMail is a fantastic email app, but improvements are always possible. Here are a few things I’d love to see implemented:

* **No viewing protection measure enabled by default.**ProtonMail should enable PIN protection by default, instead of letting it sit as a preference for users to find and use. By default, once you’re logged into your ProtonMail account on the iOS app, you’re logged in forever. For an email service that prides itself on being secure, this is an oversight that can and should be corrected.
* **Metadata**. No matter how secure ProtonMail may be, it can’t prevent your metadata from being seen by those seeking to digitally track you. Communications between two ProtonMail users might be a bit more secure but any encrypted emails that you send off-system will have metadata that’s still exposed.

## Runner Up: FlowCrypt — Updated 2021



A bonus service to consider…

I’d originally written about EasyCrypt, a secure software service for Gmail that has been discontinued. What I use and recommend now [2021] is [FlowCrypt](https://flowcrypt.com/), an implementation of PGP on the Gmail platform. That makes it an ideal solution for those users who don’t wish to have yet another email address on another platform like ProtonMail.

FlowCrypt offers a [free and paid tier](https://flowcrypt.com/pricing), easy [installations](https://flowcrypt.com/download) via browser extensions or smartphone apps, and a [decent help pages](https://flowcrypt.com/docs/). However…

As is the case with ProtonMail, *FlowCrypt cannot hide your email metadata*. And — since Google scans everyone’s emails — that means the company will have access to your metadata, including the time all your emails were sent and the email addresses of those you choose to contact. The contents of your emails — including the attachments — will not be seen by Google, which is great. But, it’s worth understanding what IS revealed by FlowCrypt and other PGP solutions, so you’ll be best prepared.

# An Important Postscript

Digital tools change frequently in response to the constant erosion of privacy, as well as the ever-changing nature of technology. It’s best to save one or more websites that will do the hard work of keeping their guidelines and recommendations up to date.

For me, one of the very best is the surveillance and self-defense project from **The Electronic Frontier Foundation or EFF**. The EFF has been [on the frontlines of digital security, user privacy, and free expression](https://www.eff.org/about) for almost thirty years — an eternity in the tech world. Their guide to safe communication is updated regularly and is required reading for those looking to stay ahead of the curve. Ditto for [PrivacyTools.io](https://www.privacytools.io/).

## [Surveillance Self-Defense](https://ssd.eff.org/" \t "_blank)

[Tips, Tools, and How-tos for Safer Online Communications](https://ssd.eff.org/" \t "_blank)

[ssd.eff.org](https://ssd.eff.org/" \t "_blank)

## [Privacy Tools | Encryption against global mass surveillance](https://www.privacytools.io/" \t "_blank)

[You are being watched! Knowledge, encryption and privacy tools to protect you against global mass surveillance.](https://www.privacytools.io/" \t "_blank)

[www.privacytools.io](https://www.privacytools.io/" \t "_blank)