Choosing the Proper Tool for the Task

Assessing Your Encryption Options

Elle Armageddon

March 21, 2017

Contents

So, you've decided to encrypt your communications. Great! But which tools are the best? There are several options available, and your comrade's favorite may not be the best for you. Each option has pros and cons, some of which may be deal breakers—or selling points!—for you or your intended recipient. How, then, do you decide which tools and services will make sure your secrets stay between you and the person you're sharing them with, at least while they're in transit?

Keep in mind that you don't necessarily need the same tool for every situation; you can choose the right one for each circumstance. There are many variables that could affect what constitutes the "correct" tool for each situation, and this guide can't possibly cover all of them. But knowing a little more about what options are available, and how they work, will help you make better-informed decisions.

Signal

Pros: Signal is free, open source, easy to use, and features a desktop app, password protection for Android, secure group messages. It's also maintained by a politically-conscious nonprofit organization, and offers: original implementation of an encryption protocol used by several other tools,[1] ephemeral (disappearing) messages, control over notification content, sent/read receipts—plus it can encrypt calls and offers a call-and-response two-word authentication phrase so you can verify your call isn't being tampered with.

Cons: Signal offers no password protection for iPhone, and being maintained by a small team means fixes are sometimes on a slow timeline. Your Signal user ID is your phone number, you may have to talk your friends into using the app, and it sometimes suffers from spotty message delivery.

Signal certainly has its problems, but using it won't make you LESS secure. It's worth noting that sometimes Signal messages never reach their endpoint. This glitch has become increasingly rare, but Signal may still not be the best tool for interpersonal relationship communications when emotions are heightened![2] One of Signal's primary problems is failure to recognize when a message's recipient is no longer using Signal. This can result in misunderstandings ranging from hilarious to relationship-ending. Additionally, Signal for Desktop is a Chrome plugin; for some, this is a selling point, for others, a deal breaker. Signal for Mac doesn't offer encryption at rest,[3] which means unless you've turned it on as a default for your computer, your stored saved data isn't encrypted. It's also important to know that while Signal does offer self-destructing messages, the timer is shared, meaning that your contact can shut off the timer entirely and the messages YOU send will cease to disappear.

[1] WhatsApp, Facebook Messenger's "Secret conversation," Google Allo's "Incognito mode"

[2] Of course, it's always best not to have relationship processing conversations via text at all, if you can avoid it!

[3] Encryption at rest means that your saved data is also encrypted, not just encrypted across the wire. By default, MacOS doesn't encrypt hard drives.

Wickr

Pros: Wickr offers free, ephemeral messaging that is password protected. Your user ID is not dependent on your phone number or other personally identifying info. Wickr is mostly reliable and easy to use—it just works.

Cons: Wickr is not open source, and the company's profit model (motive) is unclear. There's also no way to turn off disappearing messages.

Wickr is sometimes called "Snapchat for adults." It's an ephemeral messaging app which claims to encrypt your photos and messages from endpoint to endpoint, and stores everything behind a password. It probably actually does exactly what it says it does, and is regularly audited, but Wickr's primary selling point is that your user login is independent from your cell phone number. You can log in from any device, including a disposable phone, and still have access to your Wickr contacts, making communication fairly easy. The primary concern with using Wickr is that it's a free app, and we don't really know what those who maintain it gain from doing so, and it should absolutely be used with that in mind. Additionally, it is worth keeping in mind that Wickr is suboptimal for communications you actually need to keep, as there is no option to turn off ephemeral messaging, and the timer only goes up to six days.

Threema

Pros: Threema is PIN-protected, offers decent usability, allows file transfers, and your user ID is not tied to your phone number.

Cons: Threema isn't free, isn't open source, doesn't allow ephemeral messaging, and ONLY allows a 4-digit PIN.

Threema's primary selling point is that it's used by some knowledgeable people. Like Wickr, Threema is not open source but is regularly audited, and likely does exactly what it promises to do. Also like Wickr, the fact that your user ID is not tied to your phone number is a massive privacy benefit. If lack of ephemerality isn't a problem for you (or if Wickr's ephemerality IS a problem for you), Threema pretty much just works. It's not free, but at $2.99 for download, it's not exactly prohibitively expensive for most users. With a little effort, Threema also makes it possible for Android users to pay for their app "anonymously" (using either Bitcoin or Visa gift cards) and directly download it, rather than forcing people to go through the Google Play Store.

WhatsApp

Pros: Everyone uses it, it uses Signal's encryption protocol, it's super straightforward to use, it has a desktop app, and it also encrypts calls.

Cons: Owned by Facebook, WhatsApp is not open source, has no password protection and no ephemeral messaging option, is a bit of a forensic nightmare, and its key change notifications are opt-in rather than default.

The primary use case for WhatsApp is to keep the content of your communications with your cousin who doesn't care about security out of the NSA's dragnet. The encryption WhatsApp uses is good, but it's otherwise a pretty unremarkable app with regards to security features. It's extremely easy to use, is widely used by people who don't even care about privacy, and it actually provides a little cover due to that fact.

The biggest problem with WhatsApp appears to be that it doesn't necessarily delete data, but rather deletes only the record of that data, making forensic recovery of your conversations possible if your device is taken from you. That said, as long as you remain in control of your device, WhatsApp can be an excellent way to keep your communications private while not using obvious "security tools."

Finally, while rumors of a "WhatsApp backdoor" have been greatly exaggerated, if WhatsApp DOES seem like the correct option for you, it is definitely a best practice to enable the feature which notifies you when a contact's key has changed.

Facebook Secret Messages

Pros: This app is widely used, relies on Signal's encryption protocol, offers ephemeral messaging, and is mostly easy to use.

Cons: You need to have a Facebook account to use it, it has no desktop availability, it's kind of hard to figure out how to start a conversation, there's no password protection, and your username is your "Real Name" as defined by Facebook standards.

Facebook finally rolled out "Secret Messages" for the Facebook Messenger app. While the Secret Messages are actually pretty easy to use once you've gotten them started, starting a Secret Message can be a pain in the ass. The process is not terribly intuitive, and people may forget to do it entirely as it's not Facebook Messenger's default status. Like WhatsApp, there's no password protection option, but Facebook Secret Messages does offer the option for ephemerality. Facebook Secret Messages also shares the whole "not really a security tool" thing with WhatsApp, meaning that it's fairly innocuous and can fly under the radar if you're living somewhere people are being targeted for using secure communication tools.

There are certainly other tools out there in addition to those discussed above, and use of nearly any encryption is preferable to sending plaintext messages. The most important things you can do are choose a solution (or series of solutions) which works well for you and your contacts, and employ good security practices in addition to using encrypted communications.

There is no one correct way to do security. Even flawed security is better than none at all, so long as you have a working understanding of what those flaws are and how they can hurt you.

Elle Armageddon
Choosing the Proper Tool for the Task
Assessing Your Encryption Options
March 21, 2017

Retrieved on 22nd April 2021 from crimethinc.com

usa.anarchistlibraries.net