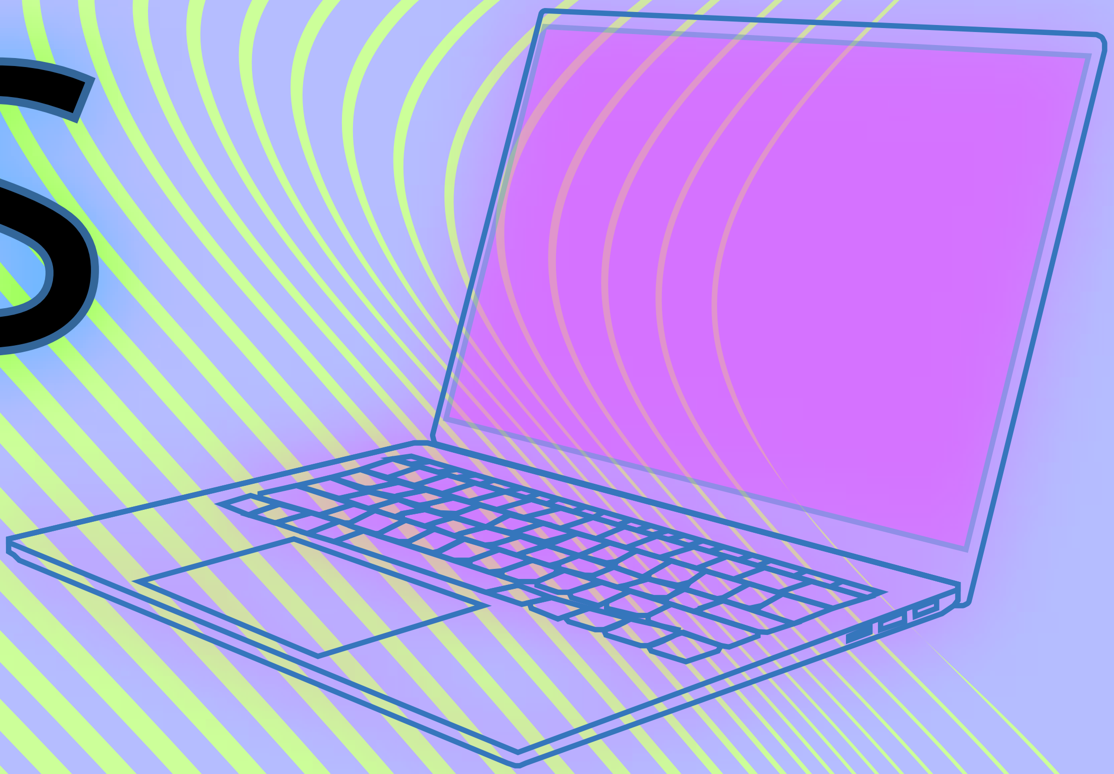
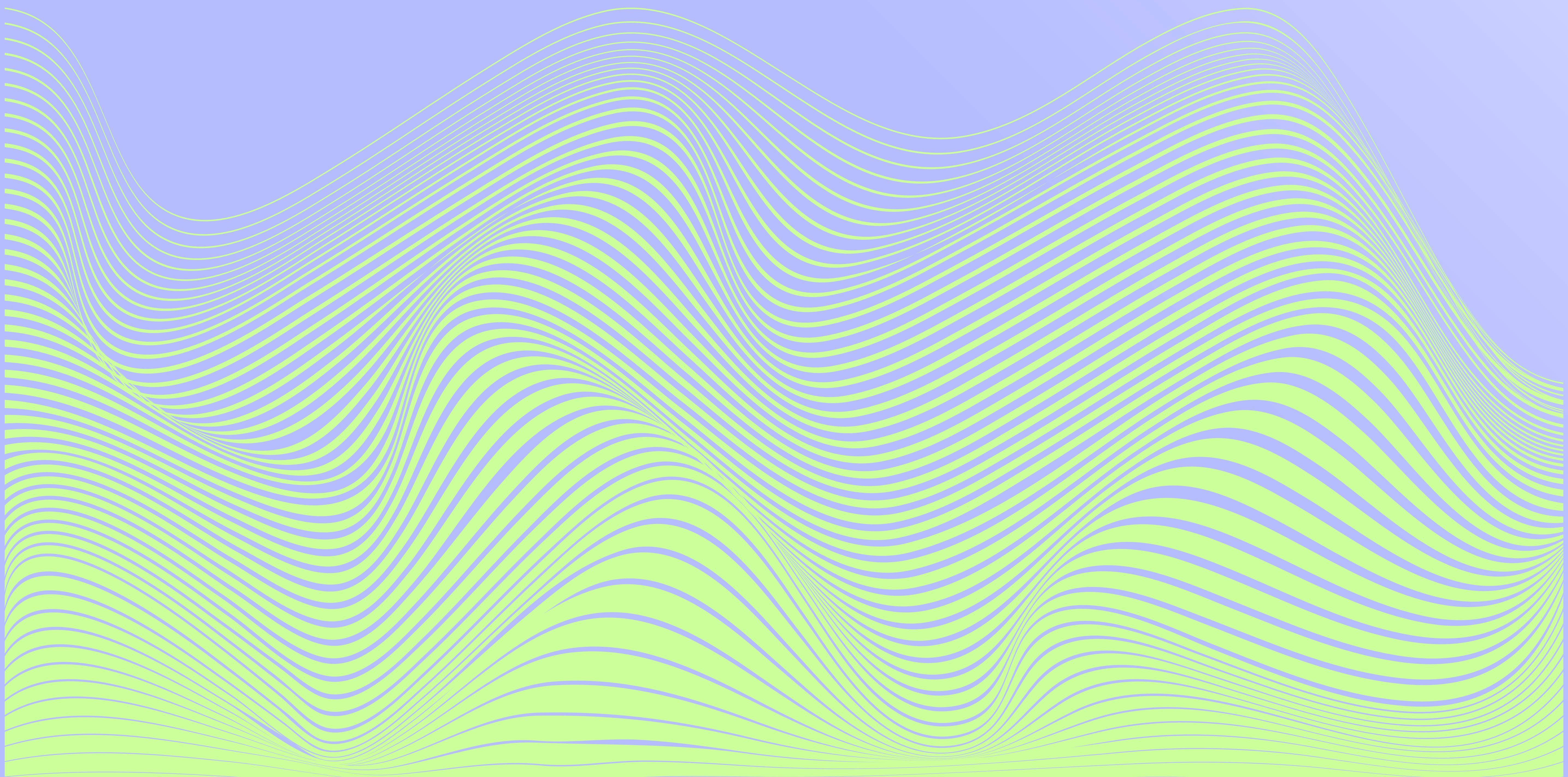
Digital Security Tools



A note on Free & Open Source Software (FOSS)

Free and Open Source Software (FOSS) is software that is usually no cost and has a non-proprietary code available for the public to review. Typically commercial software does not reveal their code because they view their software as intellectual property and a product to be sold. Downloading commercial software also assumes trust and goodwill that the company will not add a "backdoor" or a way for that company to access your private information on your device. FOSS counters this by making the code open for the public to review and analyze. Technical knowledge of coding language is needed to review but there are large enough communities of FOSS advocates, cypherpunks, hackers, and ethical developers online to catch suspicious code. FOSS is the gold standard for digital security, and the recommendations below reflect these principles.



MESSAGING

Signal is a private-messaging FOSS app for mobile and desktop devices. It employs end-to-end ecryption and is used by governments, journalist, and organizers alike to protect their communication. Signal has been transparent about government requests for their data. Sometimes tech companies get gag orders, which means the company cannot tell the public that the government has requeted their data. In these instances Signal is also protected because they have proven to the courts that they only collect 2 types of data: timestamps of accounts created, and the date each account has last connected to Signal.

“The only way to protect data is to not collect it.”
   - Mededith Whittaker, Signal President, at SXSW

Signal's additional digital-security-rock-star features include verifying a safety number, setting disappearing messages, and having usernames to remain anonymous in chats. While you may remain anonymous in chats, Signal still collects your phone number. For a step-by-step guide to set up your Signal account with a second number, please follow The Freedom of Press Foundation's, “So you want a second Signal account.” An important note is that Signal is set up for privacy, not true anonymity. For example, whether its through Google Voice, a burner app, or traditional phone company, your phone service provider (and potentially a government who is ordering them to hand over the data) can often tie your phone number to you.

Signal

SHARED DOCS

CryptPad.fr

CryptPad is a collaborative office suite that is end-to-end encrypted and open-source. It offers users file storage and a full suite of apps including a text editor, presentation slides, spreadsheets, and forms. Users can also collaborate and edit in real time, making this a useful replacement for Google Suite apps.
;
The most functional apps in the CryptPad Suite are Rich Text, Spreadsheet, and Form. While the user experience is not as clean as Google Suite, Cryptpad's commitment to encryption, open source, and free/low-cost service makes it a worthy digital-secure solution for organizers and rebel rousers.

PASSWORD MANAGER

KeePassXC

KeePassXC is an offline password manager that is FOSS. Commercial, cloud-based passwords managers (e.g. ones that are accessible via browser) are susceptible to cyber attacks. With any kind of password manager, online or offline, it is crucial that you remember your master password. Keep a written copy of your master password in a secure inconspicuous location, perhaps written on a phone bill or a sticky note on your rental lease. JUST REMEMBER WHERE YOU LEAVE IT! This cannot be retrieved if lost. A downside to an offline password manager is that you are unable to access on your mobile device. While not a solution   You may also want to consider downloading a portable version of KeePassXC to a USB drive. This will allow you to open the password manager via your USB drive from whichever device you are plugged into.