MySudo – Privacy App
Availability: iOS and Android devices
Price: Free and paid options
Created by: Anonyome Labs, Inc.
Website: MySudo.com
Last Reviewed: June 2020

MySudo is personal privacy app designed to disconnect online accounts and activity with personal information in order to increase privacy and security. The app can be used to talk, text, email, browse, and make purchases privately and securely through profiles that protect the user's private information. Users create profiles within the app called Sudos, which are distinct digital identities that allow them to connect and manage their personal information. Sudos act as a protective layer that separates the user's personal identity from these online accounts in order to keep it private and safe. The goal of MySudo is to allow the user to take back control of the information they share anytime personal information is required.

Texting
Users can communicate with unlimited end-to-end encrypted Sudo-to-Sudo messages as well as standard SMS with non-MySudo users from each Sudo profile. Texting SMS with non-MySudo users is not end-to-end encrypted.

Emailing
Users can create customized email addresses that they can use to receive and send emails with anyone around the world. Sudo-to-Sudo emails are end-to-end encrypted.

Voice Calling
Users can select a phone number with any available area code to make and receive voice calls. Users can also create custom voicemail greetings for each Sudo profile to receive voicemail messages. Voice calls to non-Sudo numbers are not encrypted, however, Sudo-to-Sudo voice calls are end to end encrypted.

Video Calling
Users can make and receive end-to end encrypted video calls with other MySudo users.

Virtual Cards
MySudo allows users to create virtual cards that act as a proxy between your credit card and the merchant. MySudo virtual cards can be used to securely make purchases with US-based merchants using the virtual card's details (i.e. 16 digit card number, expiration date, and CVV) instead of using a real personal credit card, thus keeping your credit details safe and secure. Due to federal regulations, users cannot conceal their identity when using this feature. Users must verify their identity with a proof of a physical address and cannot use a P.O. Box. This can minimize the possibility of someone misusing this feature as a tactic of abuse. To learn more: Why is MySudo asking for my real personal information for virtual cards? This feature is only available for paid subscriptions.

Subscription Plans
Sudo-to-Sudo communications are free and unlimited on any plan. Users can choose from three paid plan options, depending on how many profiles the user needs.

Privacy and Safety Considerations and Tips:

   Although users have the ability to create anonymous profiles, this does not mean that the user's device is protected from being monitored. If you think your device could be monitored by someone remotely using spy software/Stalkerware having this type of resource on your phone may be a safety risk depending on what you're using it for. For example, if the users' purpose of using MySudo is to search for domestic violence services or to connect with an advocate to safety plan, this app cannot conceal those conversations from Stalkerware or any other form of monitoring that allows the person to access the activity on the device itself. Additionally, although the calls are end-to-end encrypted, this will only prevent the interception of conversations. It will not stop someone from listening in on the conversations if the device itself is compromised with Stalkerware.
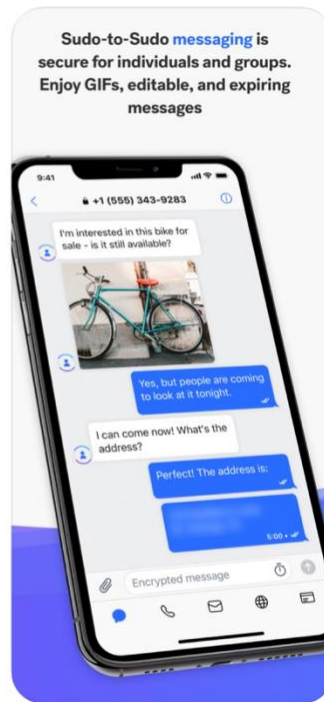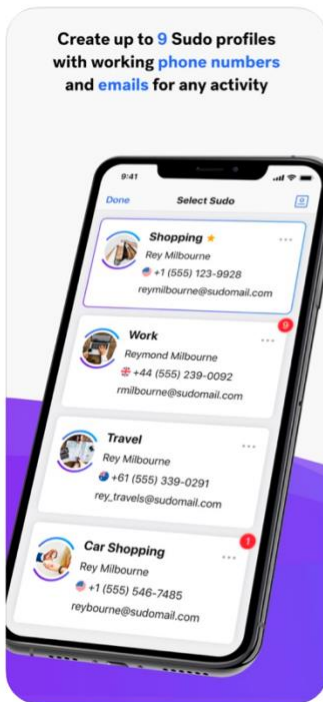
1.   If users are concerned about the possibility of someone physically looking through their device to monitor their call log, they can update the settings in the app to remove that feature. *Tap MySudo Menu, go to Settings, Calls, tap Show Calls in Recents to disable.* It's important for survivors to know that by default, calls made through MySudo will be logged.

2.   Users have the option of backing up their MySudo account via iCloud or iTunes for iOS devices and with a standard backup via their Android device. A Recovery Password in the MySudo settings must be created first before a backup is performed. This is an option in case the user wants to ensure the account will recoverable for any reason. **As a precaution, users should reconsider using this feature if someone else may have access to their iCloud account**. Please take a look at our Top 4 Tips for Cellphone Safety. And check out these links from MySudo on How to backup/restore an iOS device and How to backup/restore an Android device.

3.   Sudo-to-Sudo communications are end-to-end encrypted but users should always take precaution when connecting to open Wi-Fi.

4.   If sending photos or videos via email or SMS, it is important to remember that, depending on settings, photos and videos can collect identifiable information such as location and the date and time it was taken. MySudo **does not** remove that information from photos once uploaded. If you are concerned about your privacy, make sure that the geotag feature is turned off before the picture is taken and shared through the app. To learn more about what data/metadata is stored, please take a look at this chart located on MySudo Data and Metadata collection and storage.

5.   You can add a PIN to your MySudo app, however; the MySudo Support Team cannot retrieve the password for you if it is forgotten as that information is not stored. It is also important to ensure your device settings are set to Auto-Lock after a short period of time in case the device is left unattended. For increased privacy, we recommend that

you log out of accounts with sensitive information when not in use. If using a code, select one that someone close to you cannot guess and only you know. MySudo does not offer a login/logout feature. If it is safe, consider enabling Face ID / PIN in the MySudo Settings.

6.   Sudo-to-Sudo messaging allows text messages to be edited and even deleted after they are sent. If you are concerned that someone you are messaging with could possibly alter a text thread, consider, if it is safe to do so, taking a screenshot of the message and emailing it to an account that is not being monitored. The original unaltered text cannot be recovered once it has been edited or deleted. For more information visit: Editing a sent Sudo-to-Sudo text and Deleting a sent Sudo-to-Sudo text.

1.   MySudo has an online discussion forum where users may discuss and share their experiences and questions around issues such as privacy and online safety. This is an open forum, survivors should not share any personal information on this platform if they do not want that information to be publicly available.

What we like:
2.   Because privacy and safety is such a concern for survivors, especially those who are relocating, this app is an option for some survivors who are looking to increase their privacy.

3.   The MySudo virtual card feature can be used strategically to make online purchases and pay bills.

4.   No personally identifying information is collected when the user accesses the browser, text, call, and email features. Users do not need to register to use the app. More about the Privacy Policy.

5.   No information is shared with third parties.

6.   For an extra layer of security, users can add a passcode to the app. This prevents others from gaining access to what is inside the app in the event that someone gets your device. Be strategic when choosing your 4-digit password, if you forget it you will not be able to retrieve it from the MySudo Support Team

7.   Sudo-to-Sudo texting, email, voice, and video calls are all end-to end encrypted, which means it is private and no one outside of the conversation can listen in or read it.

8.   Private Browsing allows users to open links from Sudo emails and texts within the MySudo browser. This allows users to search for resources and information without the

Create up to **9** Sudo profiles with working **phone numbers** and **emails** for any activity

Call and **text** anyone, setup custom voicemail boxes, ringtones, and more

Sudo-to-Sudo **messaging** is secure for individuals and groups. Enjoy GIFs, editable, and expiring messages
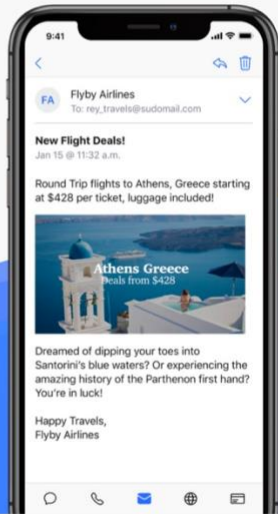
worry of their search history,

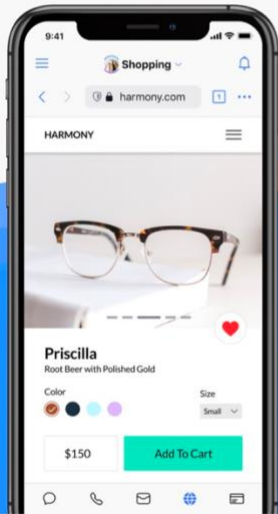bookmarks, and tabs showing up in the devices default browser.

Sudo-to-Sudo **voice** and **video** are always private and encrypted

Take control over your **email** with a **new inbox** for each Sudo

Each Sudo has a **private browser** with bookmarks, tracker blockers and more

Create **virtual cards** to protect your financial information. Shop more securely online