UBINODES

RESEARCH

SEMAPHOR APP

Review: Semaphor App.

The Semaphor app, developed by SpiderOak, allows users to securely message, chat, and share files through robust encryption. This ensures that information transfer remains confidential, eliminating the risk of eavesdropping.

Disclaimer : We are not affiliated with any of the companies mentioned. This article is based entirely on our independent findings, and there is no affiliate marketing associated with the links provided for your convenience.

How we write our reviews: To guarantee an unbiased and comprehensive review, all apps undergo testing:

• In real time, meaning they are used on real projects.

• By various team members situated in different countries.

• Across different devices and operating systems.

• For a minimum of two weeks, with an average duration of four weeks.

• The article undergoes peer review by other team members before being sent to the app's publisher for the final review.

1. Our specifications sheet:

- End to end, zero knowledge encryption (note 01).
- OpenSource (note 02).
- Administration of users (note 03).
- Resistance to state-sponsored criminals (note 04).
- Cost Effective for a large user base (note 05).
- Multiplatform (note 06).
- Own business domain (note 07).

Semaphor, a leading collaboration tool developed by SpiderOak, caters to both personal and business needs. SpiderOak has built a strong reputation among users concerned about spyware and malware, largely due to its reliable encryption.

2. Advantages of using Semaphor:

- It features a zero knowledge central server, encrypting data as it passes through (note 01).
- No passwords are required for ease of use.
- Every message and shared file is securely encrypted; the chat is encrypted before reaching other users (note 01).
- The source code is open for review (note 02 and screenshot 01).

- Semaphor offers unlimited teams and channels, allowing users to simultaneously upload multiple files.

- Semaphor Screenshot](screenshot02.png
- Users can begin downloading a file even before it completes uploading from another user's device.
- Access to channels is invitation-based, and users only see channels they are invited to (note 03 and screenshot 03).
- Channel members can be removed as needed (Screenshot 04).
- The app is accessible on both desktop and mobile devices (note 06). Users can create public groups and set auto accept for join requests (note 03 and screenshot 05).
- Users can remain anonymous by joining with either an email address or a username. The platform retains messages for 30 days before automatic deletion.
- Bots and integrations are supported based on user needs.
- A builtin search engine is provided (note 08 and screenshot 06).
- Adding a new device is convenient with the bar code scanning feature (note 09 and screenshot 07).
- Verification of addressees is facilitated through device fingerprinting (note 10 and screenshot 08).
- Updating profile settings reflects across all devices (Screenshot 09).
- It ensures consistent features across all operating systems, eliminating the need for adaptation when switching (note 11).
- Semaphor offers mobile and desktop apps for Windows, iOS, and Android operating systems.

3. Disadvantages of using Sempahor:

- It lacks app locks, making it not password-protected if another user picks up the device; fingerprinting provides a solution.
- However, at $9 per user/month, it can be expensive, particularly for large groups (note 05).
- There's a limited 2 GB file support, and no notifications for join requests; users must check for new requests by navigating to "team settings."
- To notify a specific group member, you need to tag them using @username in
- the message.
- The desktop app supports message notifications, but the mobile app lacks push notifications for incoming messages; users must enter the app to check for new notifications.
- The app may not perform well on slower internet connections, potentially resulting in multiple postings of a single message.

- It is not consistently userfriendly; if the screen is not refreshed, it may display members from the previous channel instead of the current one.
- While SpiderOak emphasizes "zero knowledge," this does not extend to zero knowledge web browsing or zero knowledge backup from mobile devices. Moreover, picture uploads lack endtoend encryption, and editing them from a mobile device is not supported. The iPad app is restricted to portrait mode and does not rotate to landscape.

4. How the Security Works:

Semaphor employs a unique security approach by using a key instead of a password. This key is a sequence of randomly generated words, which enhances security by reducing the risk of user forgetfulness or hacking, including threats from state-sponsored criminals. The use of a key mitigates common vulnerabilities associated with traditional passwords.

Semaphor encrypts messages right on your device before they are sent, ensuring only the intended recipient can read them. This provides extra security by protecting your data from the moment you create it, preventing eavesdropping or interception.

The key lets you track which devices access your account. SpiderOak, dedicated to user privacy, doesn't keep any user information, making it immune to hacking. Instead of storing data, it encrypts all messages and files exchanged between users.

If your account is attacked by someone or malware, the attacker will be blocked from accessing all accounts in your organization, not just yours. This ensures that no other accounts can be compromised. Semaphor's encryption is even more secure than storing data in the cloud.

Unlike a cloud service that stores your data on remote servers, Semaphor does not store any user data. Instead, it secures data directly on your device, ensuring transmitted data is encrypted and protected.

Access in Semaphor is restricted to channels where you've been invited, ensuring the privacy of other channels. Users can maintain anonymity, identified only by a username within the group, safeguarding personal details unless voluntarily shared.

The encryption ensures that even state-sponsored criminals, who might attempt illegal access, cannot compromise your data.

5. Other ways you can protect your information:

Utilize your own web domain for online activities and ensure your VPN is not within the 14 Eyes alliance to safeguard against surveillance by countries involved in the UK-USA Agreement. These nations conduct clandestine data collection globally.

While your data may transit through their servers, initiating traffic from elsewhere can enhance your protection. The 14 Eyes alliance includes: United Kingdom, United States, Australia, Canada, New Zealand, Denmark, France, The Netherlands, Norway, Germany, Belgium, Italy, Spain, and Sweden.

Opt for private browsing available on major web browsers. This setting erases cookies, temporary files, and browsing history when the window is closed, effectively severing ties to your online activities.

Conceal your IP address using a VPN for encrypted anonymity. Avoid divulging comprehensive personal information on social networks, minimizing the risk of exposure.

6. Alternatives to Semaphor:

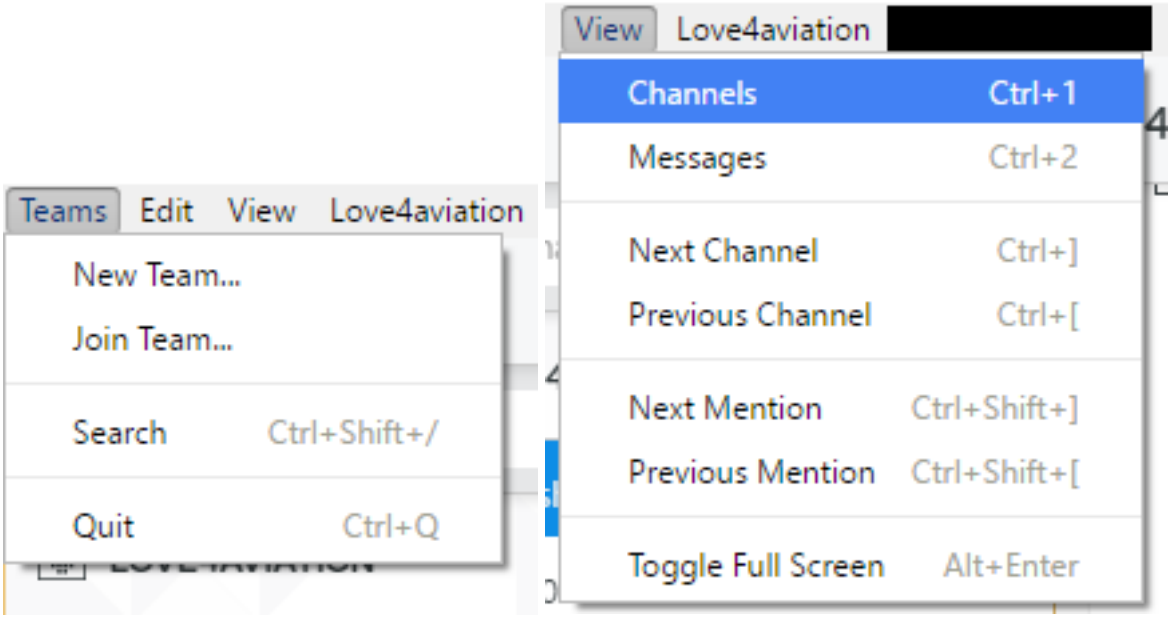
1. Alternative apps exist in the market, but none have demonstrated the same level of safety as Semaphor. Many of these apps are open source, which allows for potential modification of the original source code. While open source provides flexibility to customize the app according to specific needs, it also introduces the possibility of security enhancements, leveraging the community's ability to modify the code.
2. **Slack:** Initially popular as a secure group chat forum and still available, it lacks the "zero knowledge" cloud associated with SpiderOak.
3. **Riot:** Formerly known as Vector, Riot is an open-source app compatible with major operating systems. It offers both public and private messaging, featuring end-to-end encryption and a decentralized structure.
4. **HipChat:** A freemium service similar to Semaphor and Slack, designed for team communication within companies, includes chat history search, chat rooms, and file sharing.
5. **Mattermost:** Modeled after Slack, Mattermost is an open-source platform positioned as a cost-effective alternative. It markets itself as a Slack substitute with similar features at a lower cost.
6. **RocketChat:** Essentially a younger, open source clone of Mattermost and Slack, still in its development stages.

The alternative apps provide encrypted data options but do not offer the "zero knowledge" cloud feature provided by SpiderOak. In a "zero knowledge" cloud, SpiderOak cannot decrypt any data passing through it. This ensures that only the sender and recipient can read the data, not anyone in between. Semaphor stands out as the safest encrypted chat app because it cannot read any transmitted data, ensuring messages and shared files are securely protected between users.

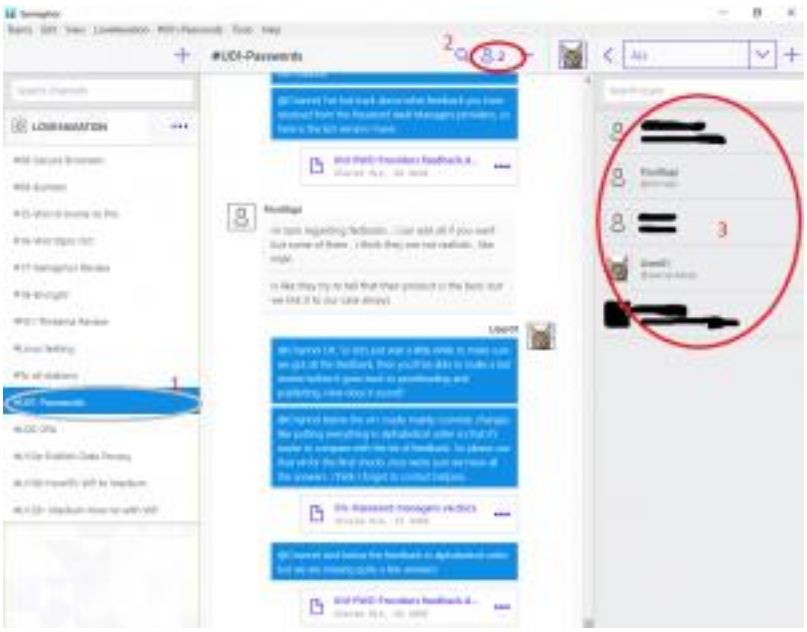
7. Screenshots:

01: Source code is also reviewable.

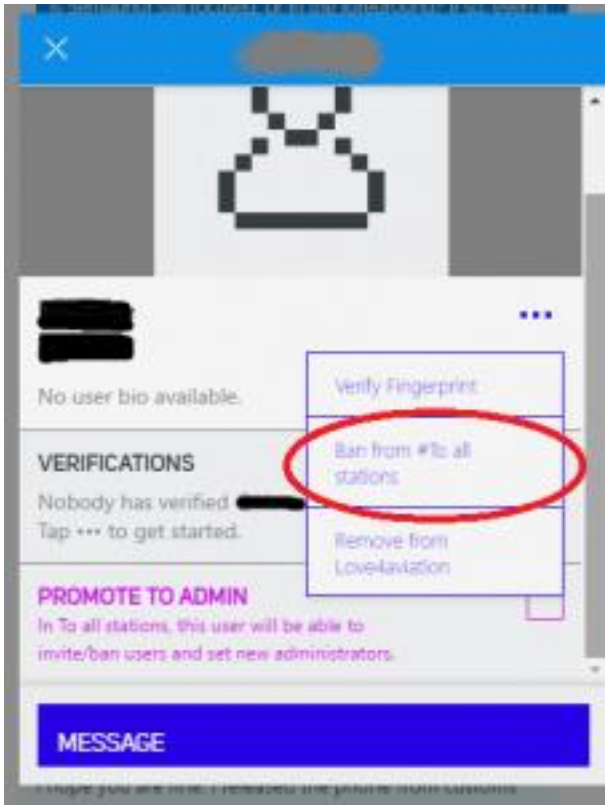
02: Unlimited teams and unlimited available channels.



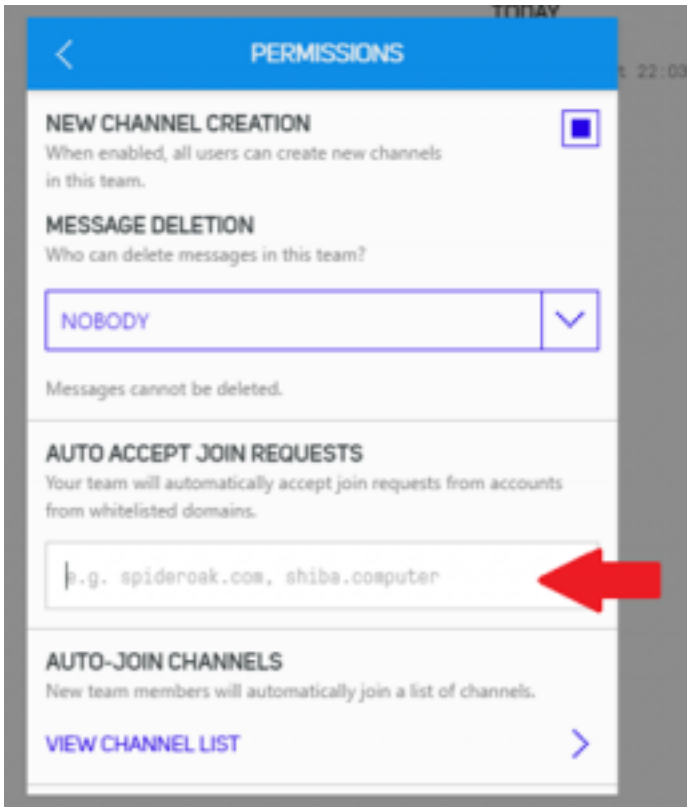
03: A user does not see all of the channels.



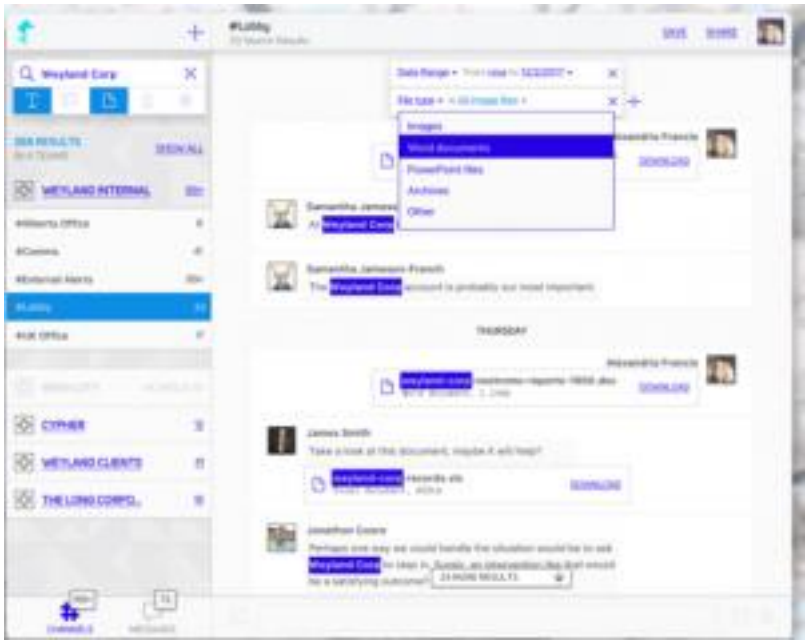
04: Remove members from a channel.



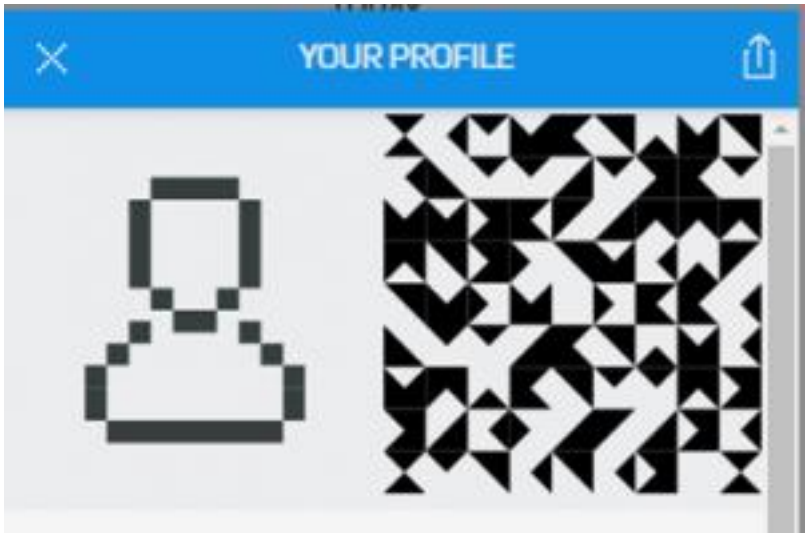
05: Allows you to create public groups as well as autoaccept any join requests.



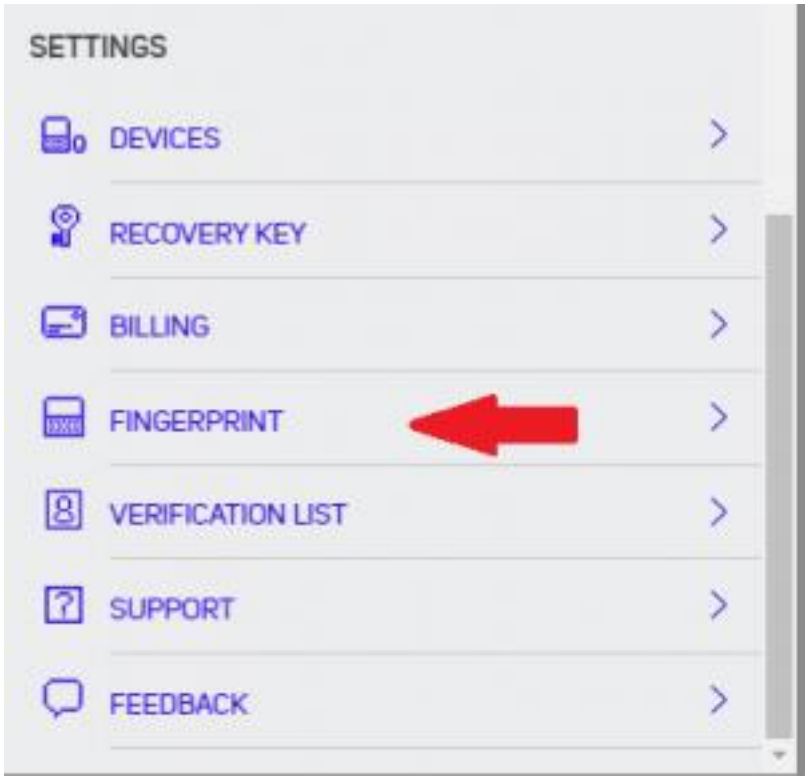
06: Builtin search engine.



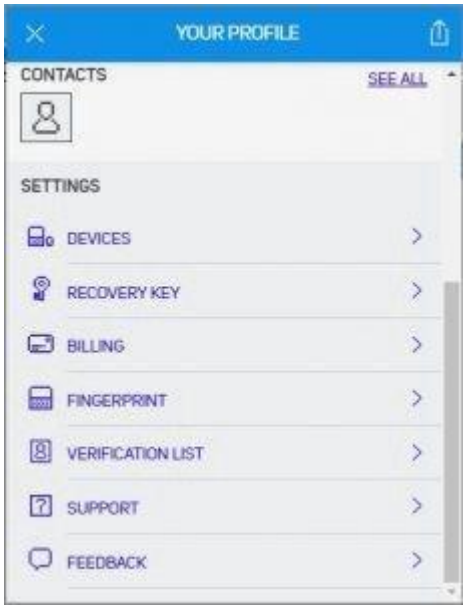
07: Add a new device with its bar code.



08: Verify addresses by fingerprinting.



09: Change your profile settings.



7. Notes:

(1) Endtoend encryption is achieved as:

No central server, data is downloaded to devices.
Every message & file is cryptographically secure.

(2) Open source code: Go to: https://spideroak.com/solutions/semaphor/source

(3) Administration of users:

Create a new team or join an existing one.

Establish multiple channels and navigate seamlessly between them.

Users can only view channels to which they are invited.

Create public teams and enable auto acceptance of join requests.

Access the "Manage Team" section and navigate to "Permissions."

(**4**) **Resistance to statesponsored criminals:** Police, prosecutors, and other officials can abuse their authority by corrupting state institutions, posing a serious threat to individuals and nations. If involved in illegal activities, they can manipulate the system to cover their tracks, intercepting and reading communications secured with IMAP, POP3, TLS, and SSL. They may even spoof your email provider's SSL certificate to gain access to SMS and emails, compromising recovery options. It's crucial to always use encryption software, secure your devices, and purchase hardware from outside your country for added protection.

(**5**) **Costeffective for large user base:** Don't meet. $9 per user/month is expensive for big teams.

(**6**) **Multiplatform:** For Desktop, Go to: https://spideroak.com/personal/semaphor For Android, you can find it in Google play.

(**7**) **Own business domain:** To minimize the risk of attacks by state-sponsored criminals targeting DNS records, host your domain in a location that emphasizes access protection. Opt for a country different from your email provider and outside the Fourteen Eyes alliance, which values privacy and democracy. Utilize end-to-end encryption to safeguard your emails against interception. These steps enhance security against potential threats to your online communications.

(**8**) **Built in search engine:** Works even offline.

(**9**) **Easy to add new device with bar code scanning:** No need to reenter credentials.

(**10**) **Can verify addressees by fingerprinting devices:** List of verified addressees in the apps settings.

(**11**) **Same features on all types of operating systems:** For example you can accept join request from a mobile device, you don't need to use the desktop app to get some admin features.

