UBINODES

REVIEW: ENCRYPTR APP.

Review: Encryptr App.

There are specific use cases where Encryptr is the best solution. We explain this in this article.

Disclaimer : We have no affiliations with the mentioned companies; this article is entirely based on our independent findings. There is no affiliate marketing associated with the provided links for your convenience.

How we write our reviews: For an impartial and comprehensive review, all apps undergo rigorous testing:

• Real-time usage on actual projects.

• Evaluation by team members from diverse locations.

• Testing across various devices and operating systems.

• Minimum two-week, typically four-week, trial periods.

• Peer review by team members, followed by submission to the app's publisher for final review.

In our article evaluating password managers for business use, we included Encryptr, despite its limitation of lacking a sharing feature suitable for groups. A detailed description of Encryptr can be found on SpiderOak's website. It's essential to note that while Encryptr may not be suitable for group usage, there are specific use cases where it stands out as the best solution.

1. Use cases:

- To transmit data anonymously.
- To back up selected credentials not intended for inclusion in your primary password manager without registering with an additional provider.
- To synchronize specific data across your devices.

2. Specifications of Encryptr:

- End-to-end, zero-knowledge encryption (Note 01).
- Open source (Note 02).
- Auto log off.
- Intuitive.
- Free.
- Cross-platform (Note 03).
- Can share notes as well.
- No recovery option.
- Offline access which is sensitive to device theft as it stores data on APPDATA folder (Note 05).

3. Example for passing on data anonymously:

Step 1:

- Create a specific login-password combination for the data you want to pass on.

Step 2:

- Give this combination to your addressee.

Step 3:

- Once the addressee has confirmed he/she has access to the Encryptr, delete it from your computer.

4. Pros and Cons in this use case:

4.1 Pros:

- Your recipient is not required to create an account with a password manager provider.
- The application is user-friendly, requiring no learning curve for your recipient.
- Encryptr is downloadable at no cost and anonymously, eliminating the need for registration with SpiderOak.
- Being cross-platform allows usage with individuals irrespective of their computer preferences.
- Not only can login credentials be shared, but also notes.
- The transfer lacks direct real-time communication between parties, reducing interception risk by minimizing communication events.
- The absence of recovery options (SMS or email) decreases the attack surface for state-sponsored criminals (Note 04).

4.2 Cons:

- Data is stored locally on your computer, which poses a potential hacking risk (Note 05). Ensure your hard drive is consistently encrypted. After concluding use with Encryptr, delete it by accessing the APPDATA folder and using a freeware tool like Privazer for Windows.

5. Notes:

(1) Zero knowledge encryption necessitates storing the key on the user's device to ensure protection against state-sponsored criminals. While this doesn't eliminate the possibility of government access to plain text messages, it would require actively hacking the user to obtain the necessary password..

(2) While open source doesn't guarantee a thorough code audit for backdoors or weaknesses, it does demonstrate a commitment to transparency. The source code of Encryptr is accessible to the public.

(3) Must be accessible on iOS, Android, Windows, Linux, and Mac desktops. Windows phones and Blackberry are excluded due to limited options, making it nearly impossible to find a compatible solution for these platforms.

(4) Police, prosecutors, and similar officials can engage in what appear to be "legal" crimes by corrupting state institutions, posing significant threats to individuals and nations alike. Their capacity to conceal illegal activities is alarming, including intercepting and reading IMAP, POP3, TLS, and SSL communications. They can also spoof your email provider's SSL certificate and gain access to your SMS and emails, turning recovery options into potential attack vectors. Therefore, it's crucial to consistently employ encryption software, secure your devices, and procure hardware from outside your operating country to mitigate these risks.

(5) There are specific software designed to crack these password managers, for example Elcomsoft: https://blog.elcomsoft.com/2017/08/one-password-to-rule-them-all-breaking-into-1password-keepass-lastpass-and-dashlane/