

How to Download End-to-End Encrypted Messenger Messages from Facebook?

Currently, you can only download your information from Facebook end-to-end encrypted chats on a computer.



You can download a copy of your end-to-end encrypted messages at any time if you've **turned on secure storage** on Facebook. ([How to turn it on?](#))

Your data in end-to-end encrypted chats can include:

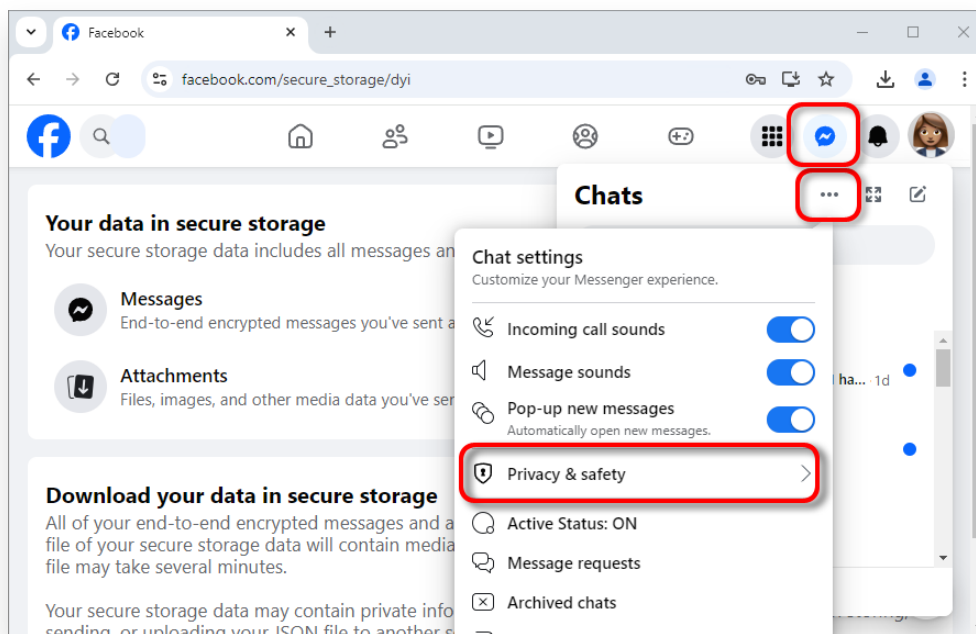
- a. Messages you've sent and received from other people.
- b. Attachments, such as files, images and other media you've sent and received.


Step 1:

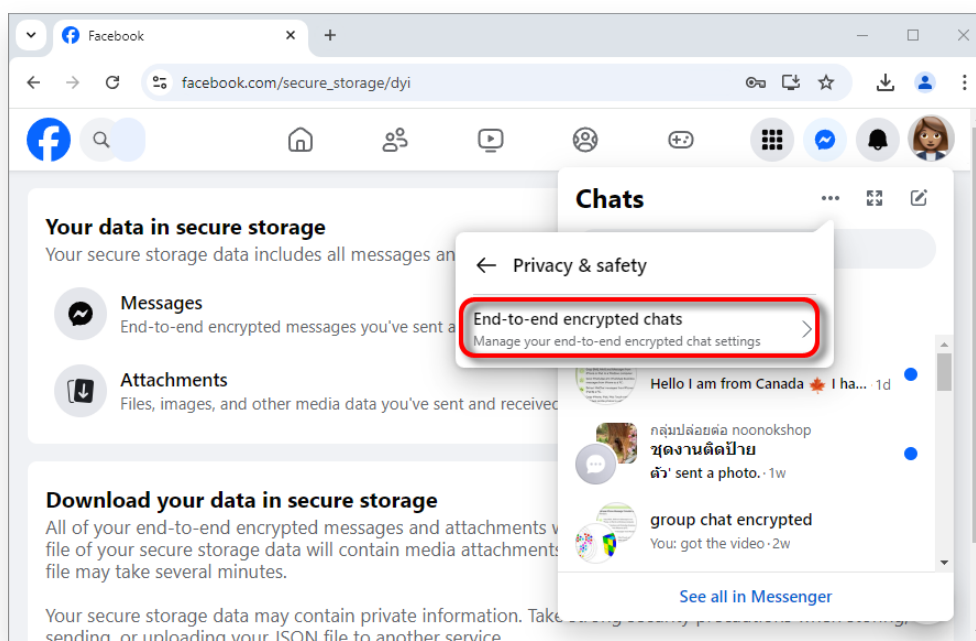
Follow the step by step guide below to download your information from secure storage:

1. On a computer, open facebook.com and log into your account. Click . Then click  (the three-dot icon) and select **Privacy & safety**.
2. Click **End-to-end encrypted chats**.
3. Click **Secure storage**.
4. Click **Download secure storage data**.
5. Click **Download file** and enter your Facebook password when prompted, then click **Confirm**.
6. Click **Download**. It may take several minutes to prepare your download file.

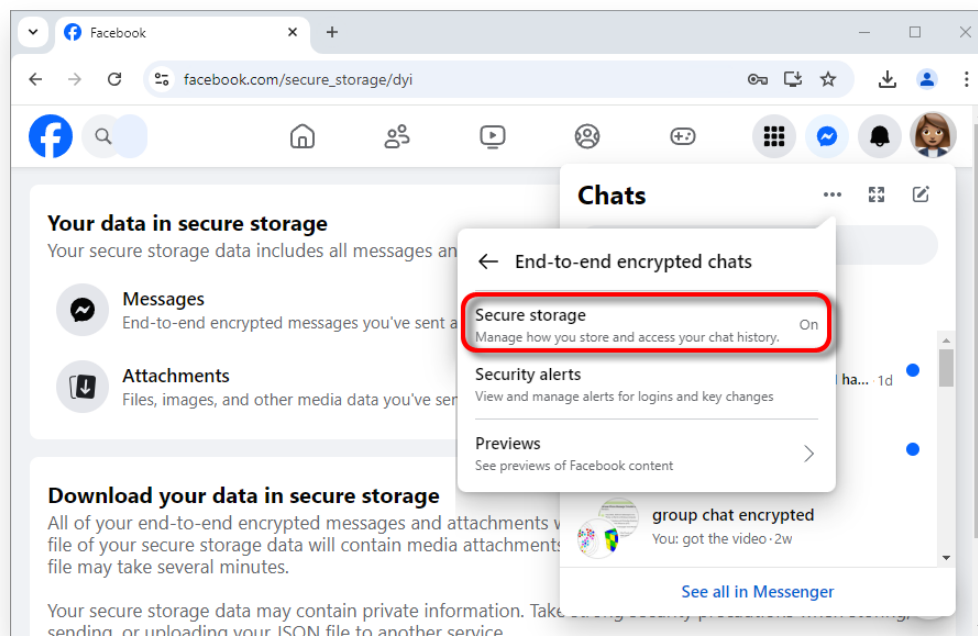
Note: All of your end-to-end encrypted messages and attachments will be formatted into a ZIP file. (The zip file is named like **messages.zip**.)



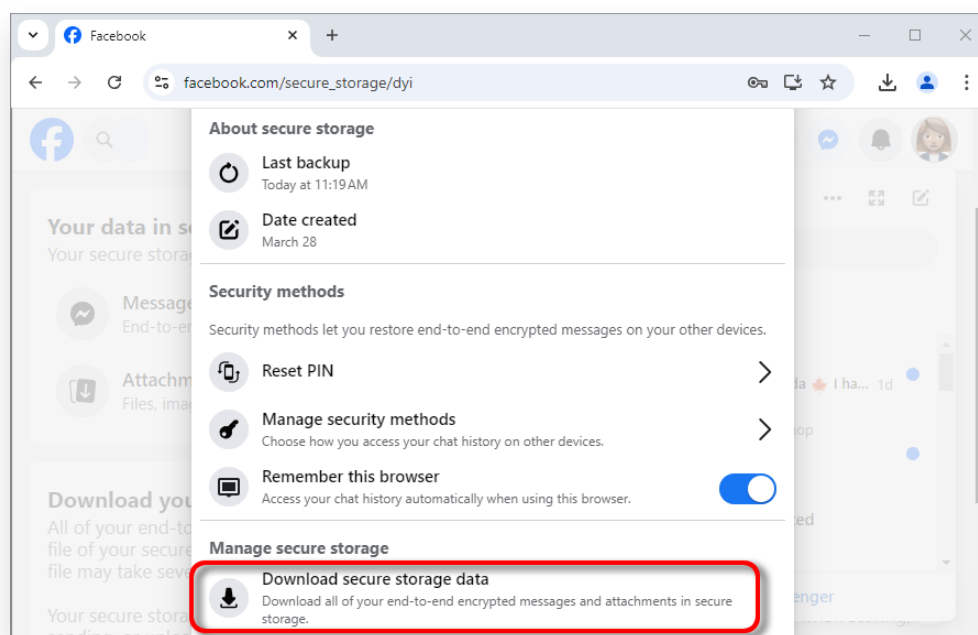
1. Click . Then click (the three-dot icon) and select Privacy & safety.



2. Click **End-to-end encrypted chats**.



3. Click **Secure storage**.



4. Click **Download secure storage data**.

Your data in secure storage

Your secure storage data includes all messages and attachments



Messages

End-to-end encrypted messages you've sent and received from



Attachments

Files, images, and other media data you've sent and received in

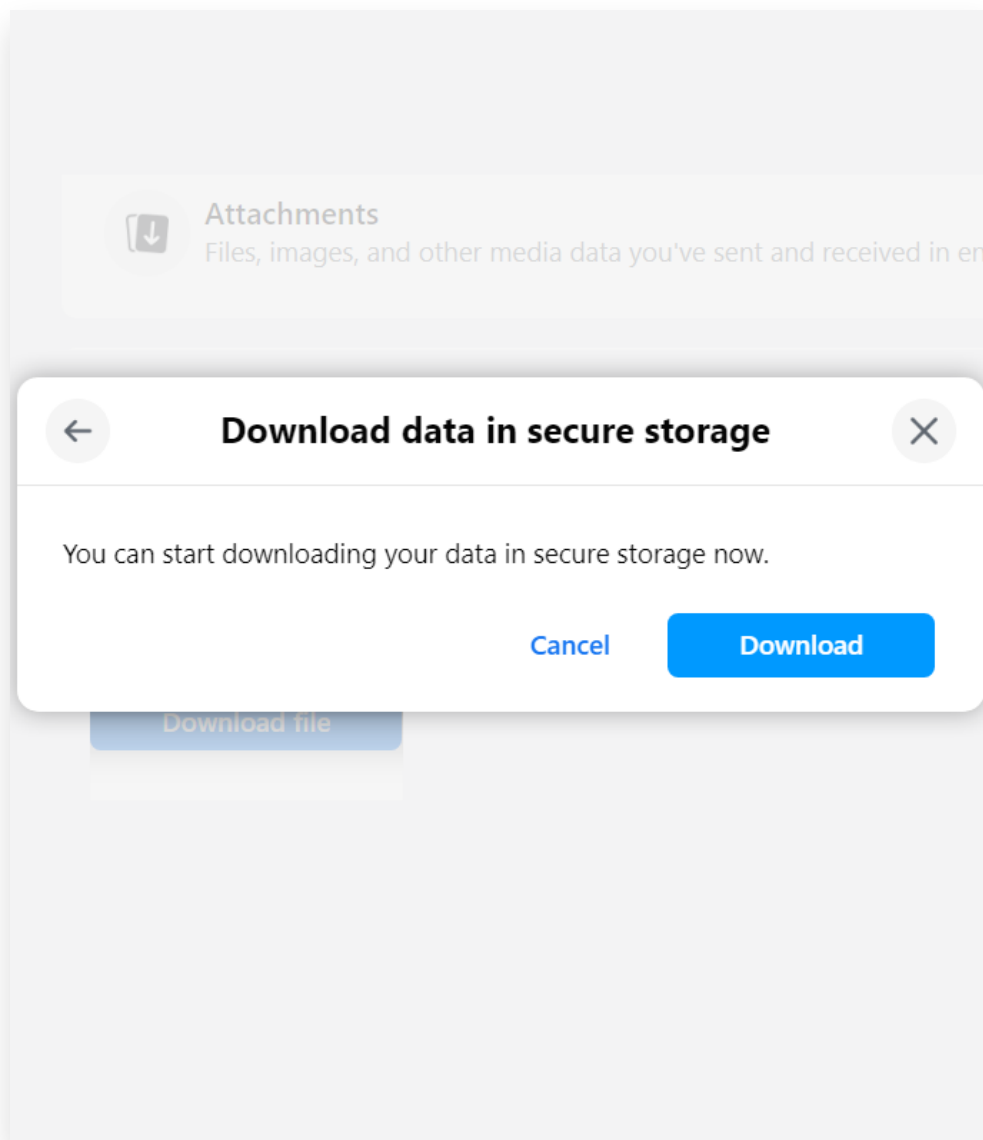
Download your data in secure storage

All of your end-to-end encrypted messages and attachments will be included in the JSON file of your secure storage data. The file will contain media attachments you've sent and received. The file may take several minutes.

Your secure storage data may contain private information. Take steps to protect it before sending, or uploading your JSON file to another service.

[Download file](#)

5. Click **Download file**.



6. Click **Download**.

**Step
2:**

Tansee iPhone Message Transfer or Tansee Android Message Transfer can extract the zip file(s) downloaded from Facebook.

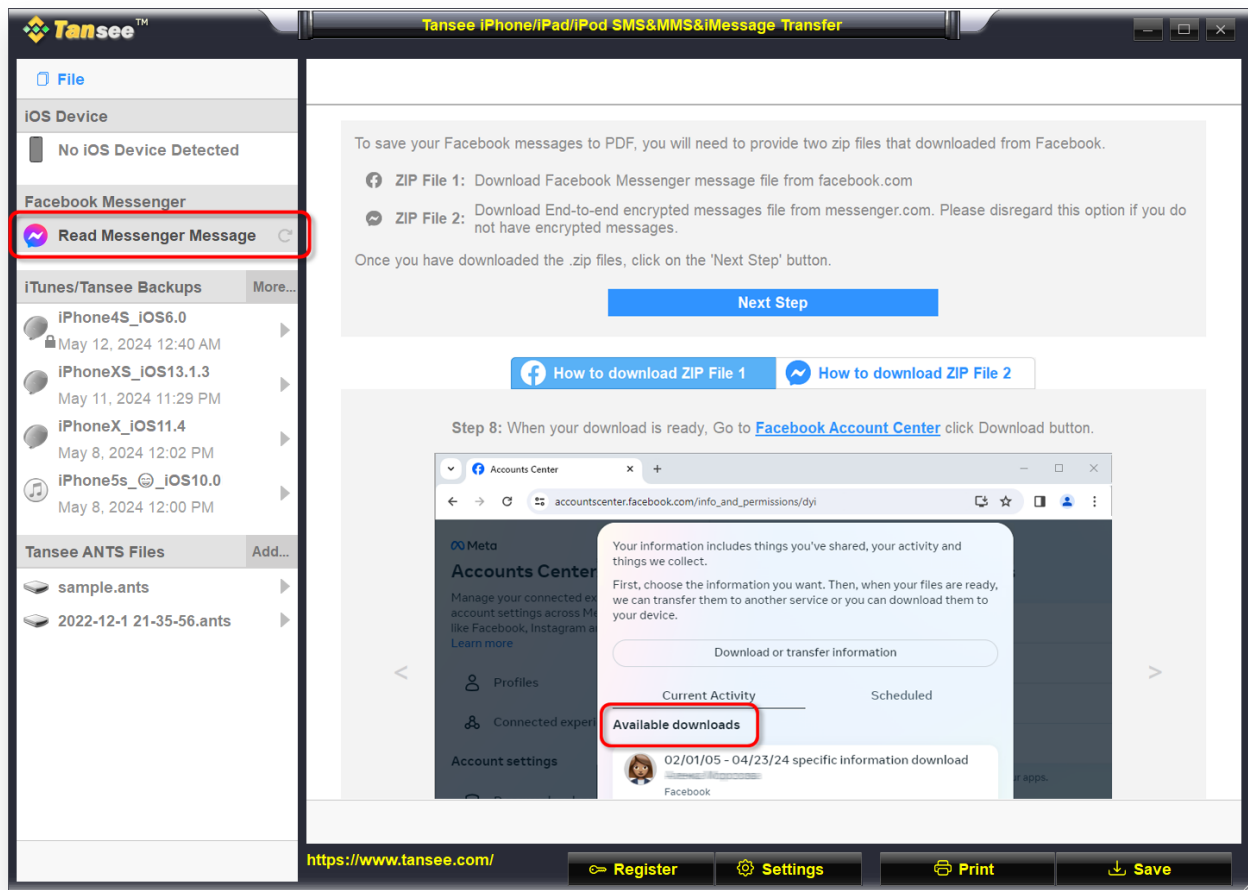
Tansee can be used to save all Facebook Messenger messages, including all attachments, as PDF files.

After downloading the zip file(s) from Facebook, please download and install the latest version of Tansee iPhone Message Transfer [here](#).

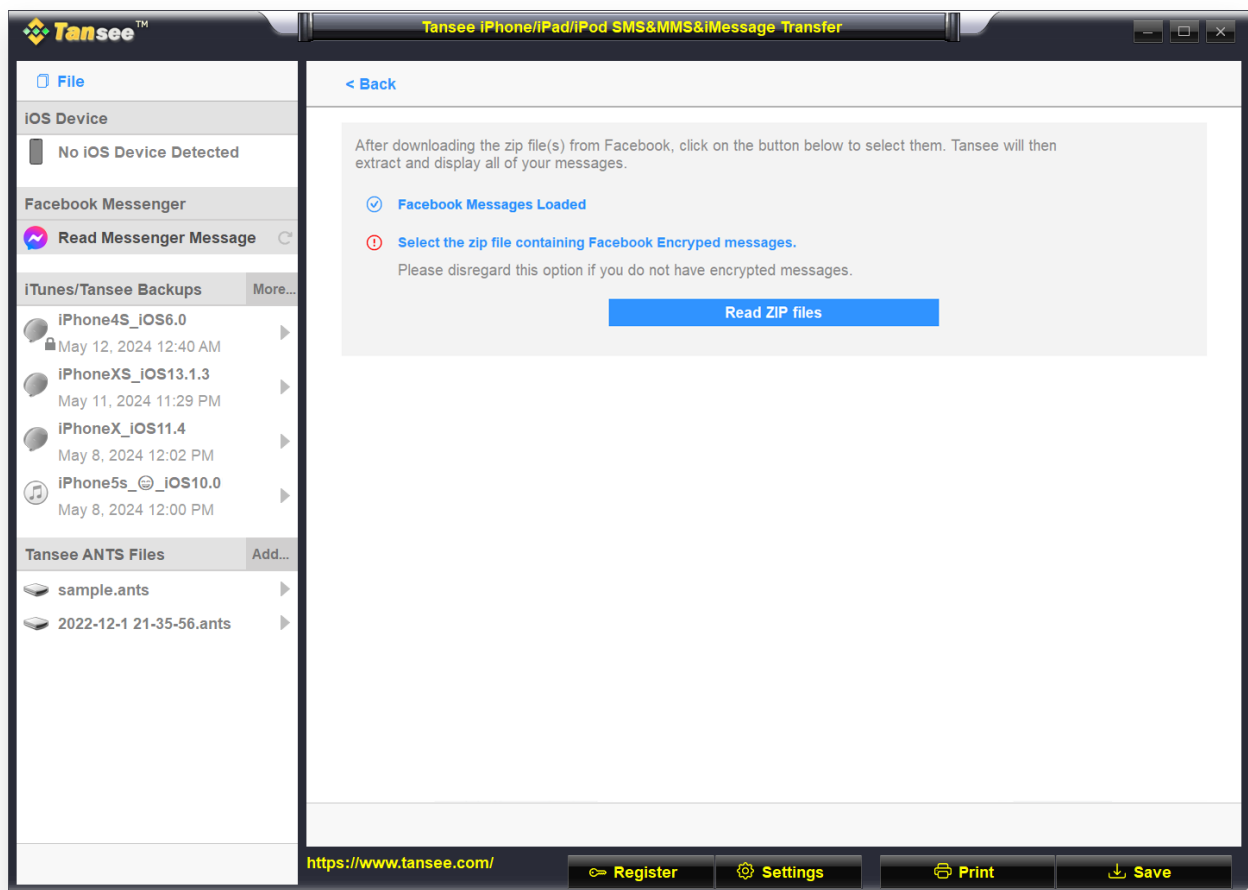
Alternatively, you can download and install the latest version of Tansee Android Message Transfer [here](#).

1. Open either Tansee iPhone Message Transfer or Tansee Android Message Transfer.
2. Click on the 'Read Messenger Messages' option.
3. Select the zip file that contains your Facebook messages.
4. Click on 'Read zip files' and Tansee will automatically extract and display all of your messages.

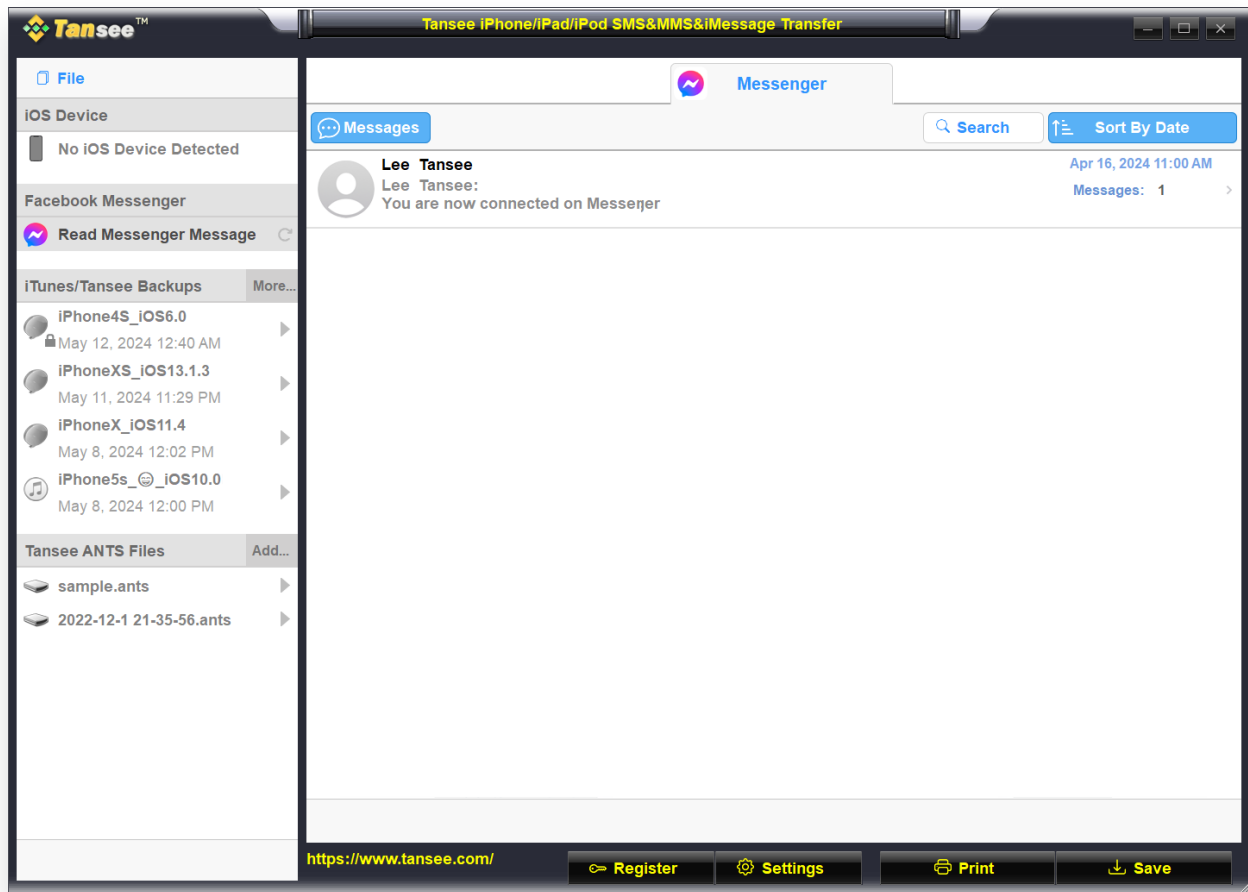
5. Once Tansee has finished reading all of your messages, click on the save button and select the PDF file format.



Click on the 'Read Messenger Messages' option.





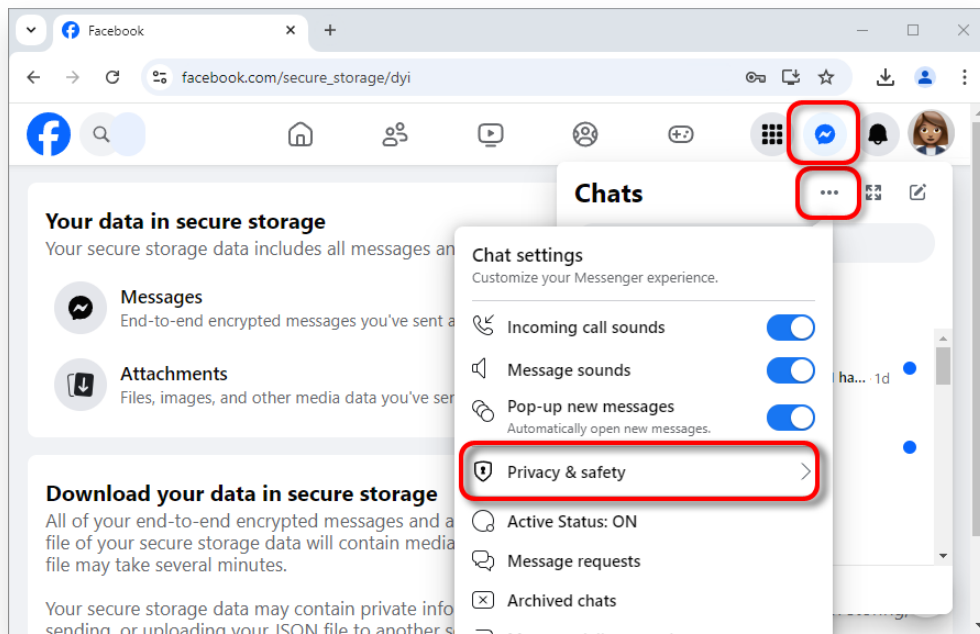
Select the zip file that contains your Facebook messages.




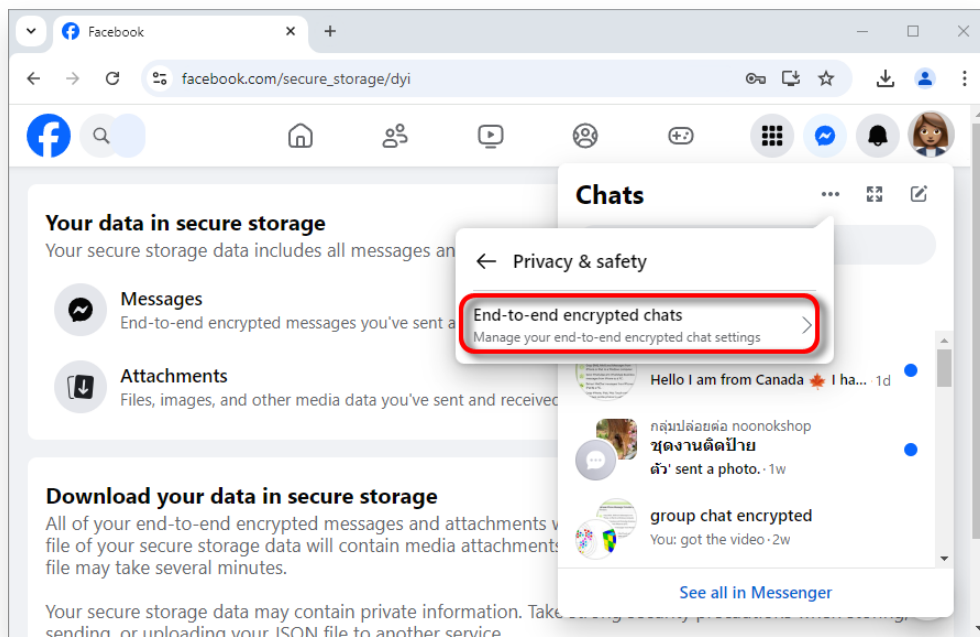
Click on 'Read zip files' and Tansee will automatically extract and display all of your messages.

? How to turn on secure storage?

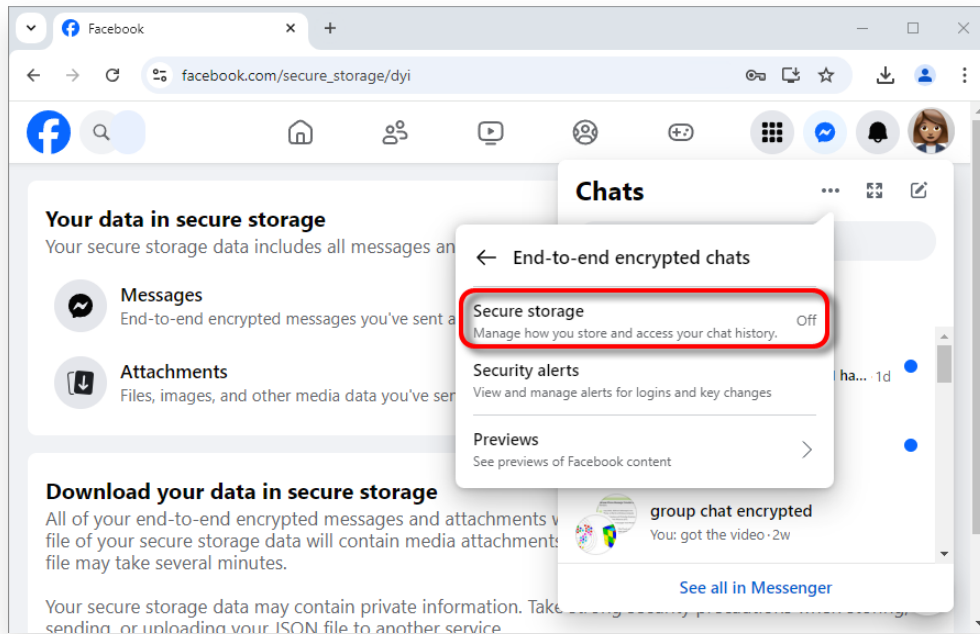
1. On a computer, open [facebook.com](https://www.facebook.com) and log into your account. Click . Then click  (the three-dot icon) and select **Privacy & safety**.
2. Click **End-to-end encrypted chats**.
3. Click **Secure storage**, then click **Turn on secure storage**.
4. **Enter your PIN**. Using a Google Account on Android mobile devices or an Apple account on iOS mobile devices will enable you to log in without needing to enter a PIN.
5. Follow the on-screen instructions. If you created a PIN, remember to keep it somewhere safe. You'll need it to restore your chats in secure storage on a new device.



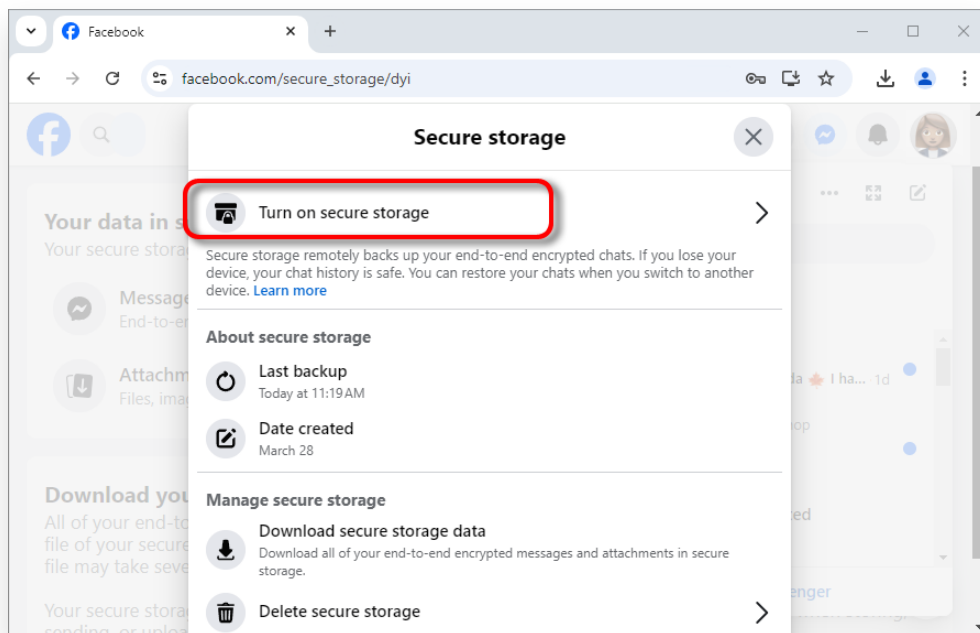
1. Click . Then click (the three-dot icon) and select Privacy & safety.



2. Click **End-to-end encrypted chats**.

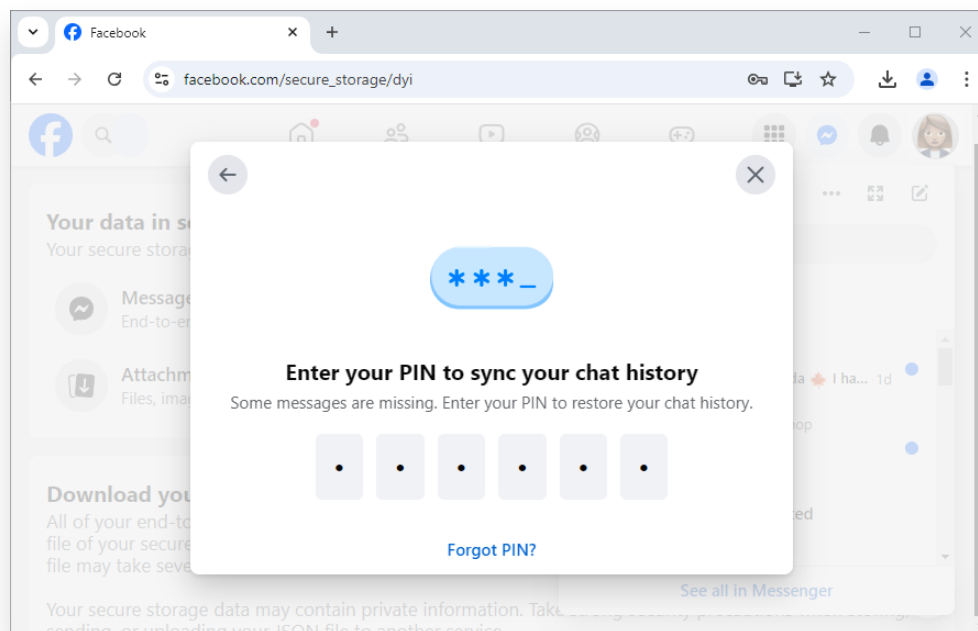


3. Click **Secure storage**.



and then click **Turn on secure storage**.





4. Enter your PIN.

? What happens if Facebook secure storage is off?

When Facebook secure storage is turned off:

You won't be able to restore your end-to-end encrypted message history if you replace your device.

Your device will stop backing up new end-to-end encrypted messages.

If you choose to delete secure storage:

Any backup of your end-to-end encrypted messages will be permanently deleted.

Messages saved on your device won't be affected.

Note: New end-to-end encrypted messages will only be stored on your device, not in secure storage.

If you decide to turn on secure storage later, all your end-to-end encrypted chats on your device will be saved to secure storage. This means that if you replace your device and use Facebook, you can restore your message history.

? What end-to-end encryption on Messenger means?

Some products don't currently support end-to-end encryption, such as community chats for Facebook groups, chats with business and professional accounts, Marketplace chats and others.

End-to-end encryption on Messenger adds extra security and protection to your messages and calls so only you and whoever you're talking to can see, hear or read them.

The content of your messages and calls in end-to-end encrypted conversations is protected from the moment it leaves your device to the moment it reaches the receiver's device.

This means that nobody else can see or listen to what's sent or said - not even Meta. We couldn't even if we wanted to.

How end-to-end encryption protects your conversation?

Every device in an end-to-end encrypted conversation has a special key to protect the conversation. When you send a message in an end-to-end encrypted conversation, your device locks the message as it's sending. This message can only be unlocked by a device that has one of the keys for that conversation.

No one can access your messages or calls except the people with the keys. You and whoever you're talking to in end-to-end encrypted conversations are the only people with unique, matching keys.



© 2006-2025 Tansee, Inc

[Home](#) [Support](#) [Privacy Policy](#)

[Affiliate](#) [Contact Us](#)