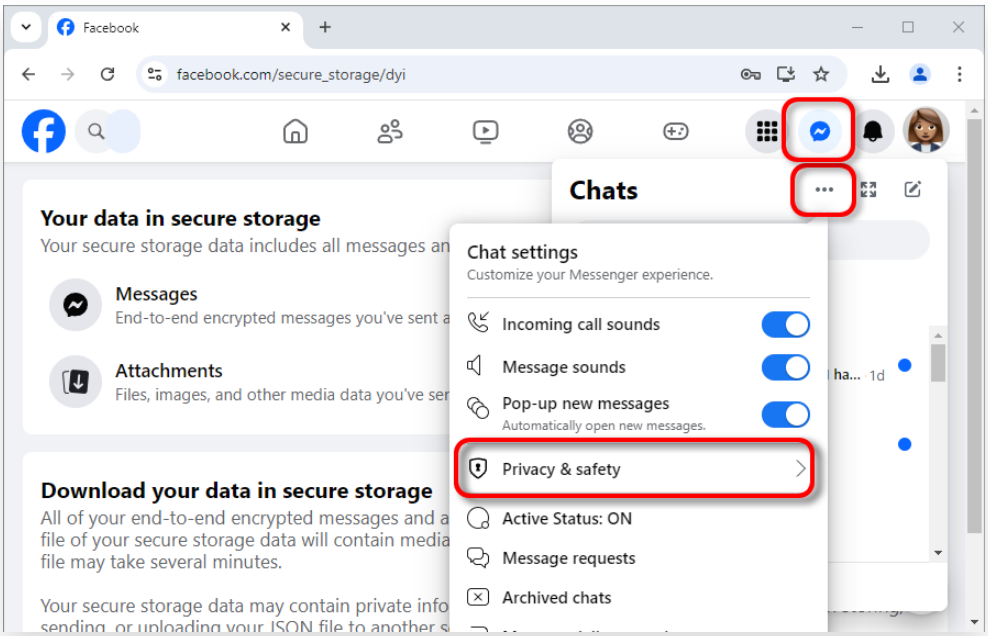
Come scaricare messaggi Messenger crittografati end-to-end da Facebook?

Al momento, puoi scaricare le tue informazioni solo dalle chat crittografate end-to-end di Facebook su un computer.
Puoi scaricare una copia dei tuoi messaggi crittografati end-to-end in qualsiasi momento se hai **attivato l'archiviazione sicura** su Facebook. (Come attivarlo?)
I tuoi dati nelle chat crittografate end-to-end possono includere:
UN. Messaggi che hai inviato e ricevuto da altre persone.
B. Allegati, come file, immagini e altri contenuti multimediali che hai inviato e ricevuto.

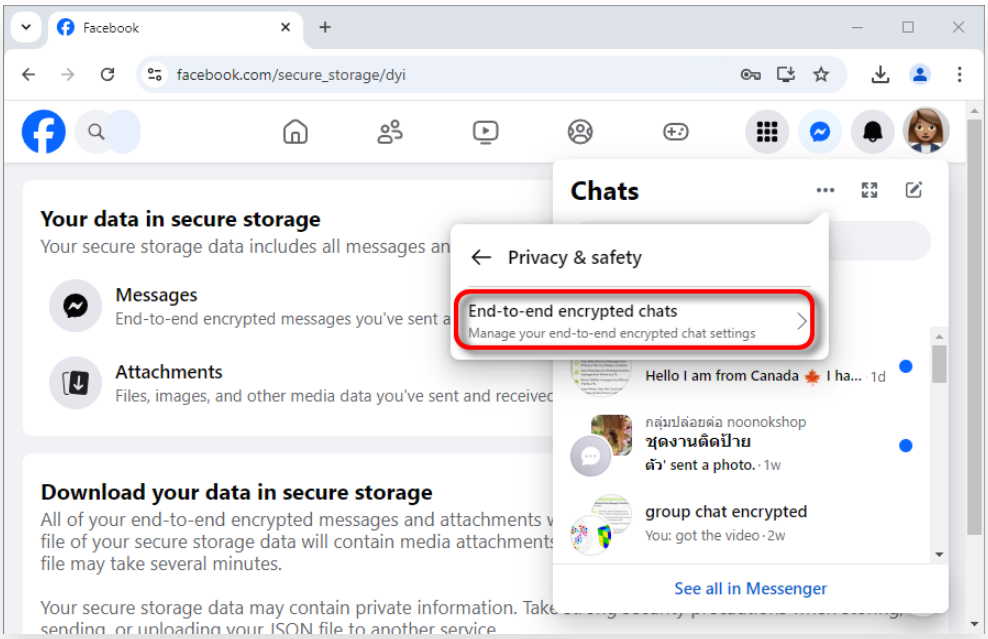
Passaggio 1: **Segui la guida passo passo di seguito per scaricare le tue informazioni dall'archiviazione sicura:**

1. 1.Su un computer, apri facebook.com e accedi al tuo account. Clic . Quindi fare clic su (l'icona a tre punti) e selezionare Privacy e sicurezza.
2. Fai clic su **Chat crittografate end-to-end**.
3. Fai clic su **Archiviazione sicura.**
4. Fai clic su **Scarica dati di archiviazione sicura.**
5. Fai clic su **Scarica file** e inserisci la password di Facebook quando richiesto, quindi fai clic su **Conferma**.
6. Fai clic su **Scarica**. Potrebbero essere necessari diversi minuti per preparare il file di download.

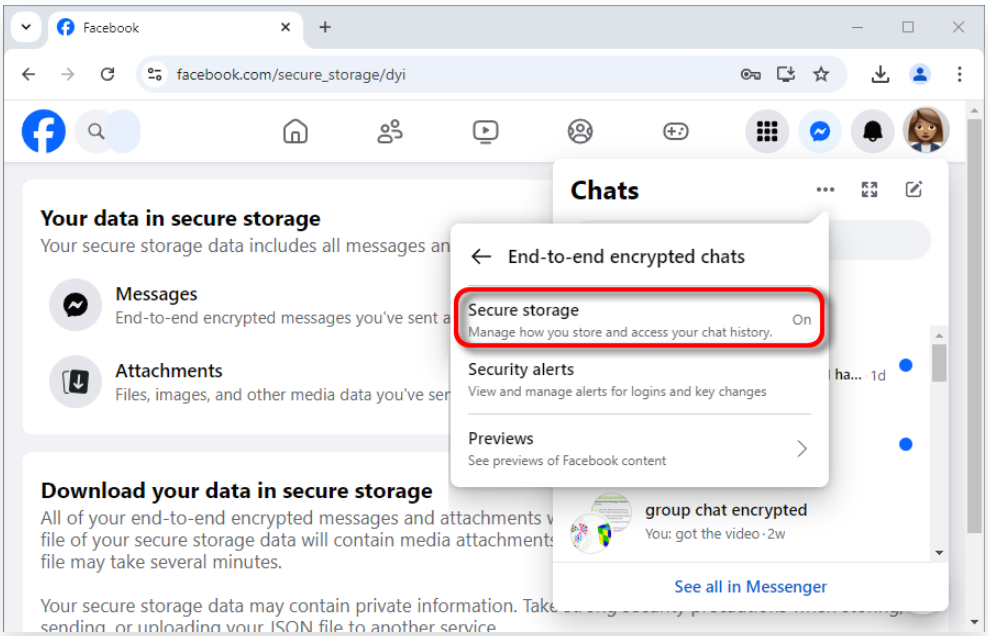
Nota: tutti i messaggi e gli allegati crittografati end-to-end verranno formattati in un file ZIP. (Il file zip ha un nome simile a **messages.zip**.)



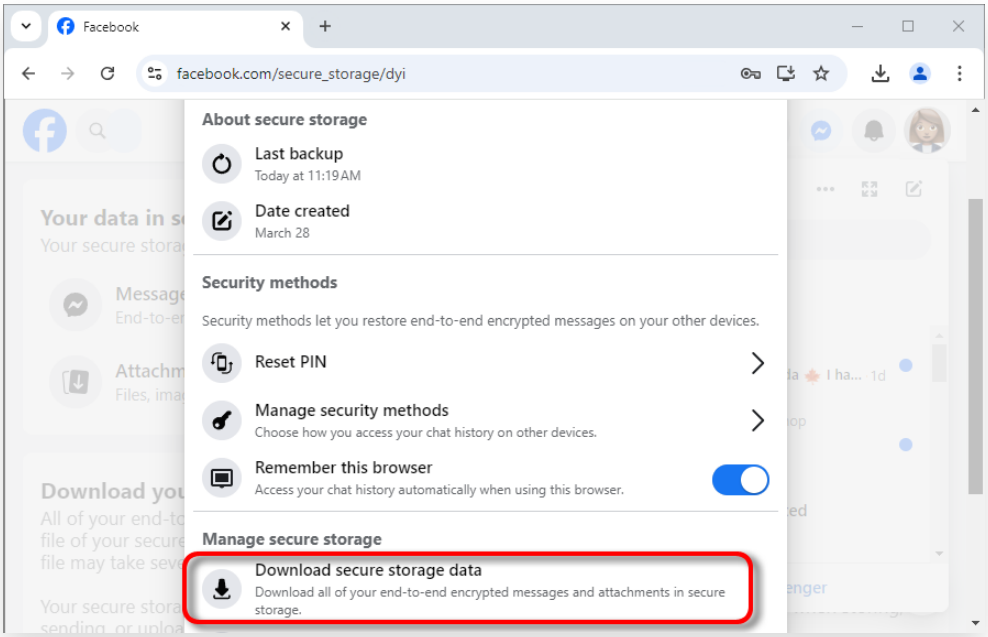
1. Clic . Quindi fare clic su (l'icona a tre punti) e selezionare Privacy e sicurezza.



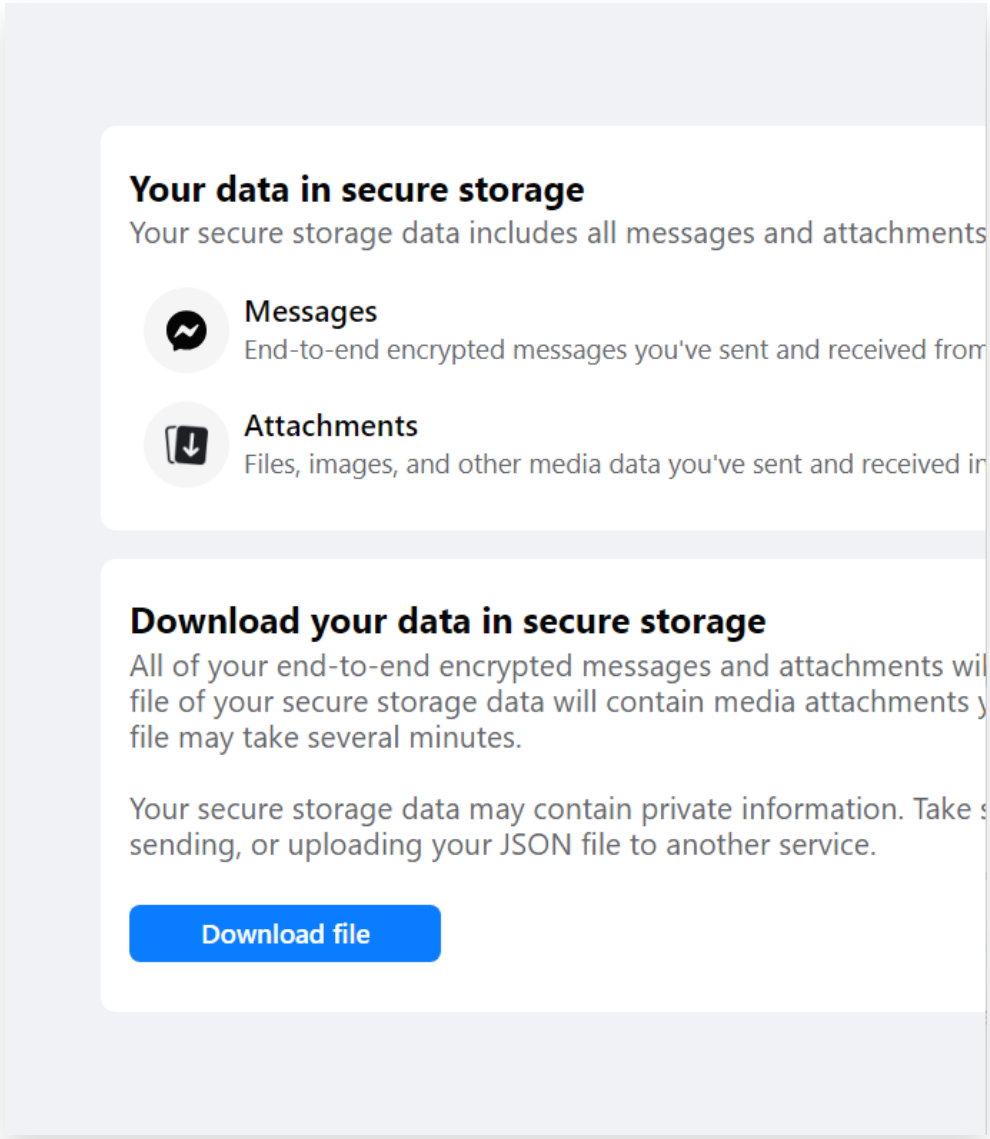
2. Fai clic su **Chat crittografate end-to-end**.



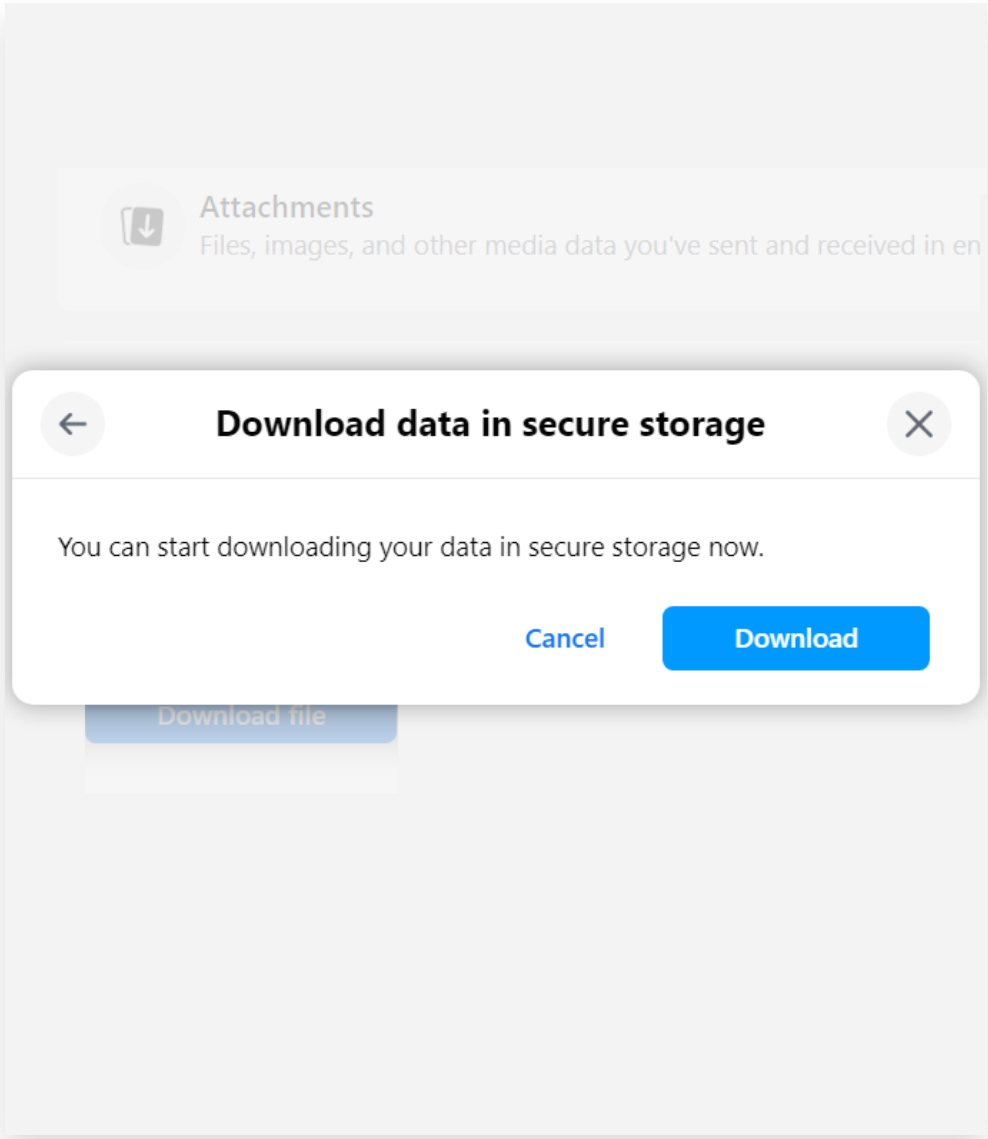
3. Fai clic su **Archiviazione sicura**.



4. Fai clic su **Scarica dati di archiviazione sicura**.



5. Fai clic su **Scarica file**.



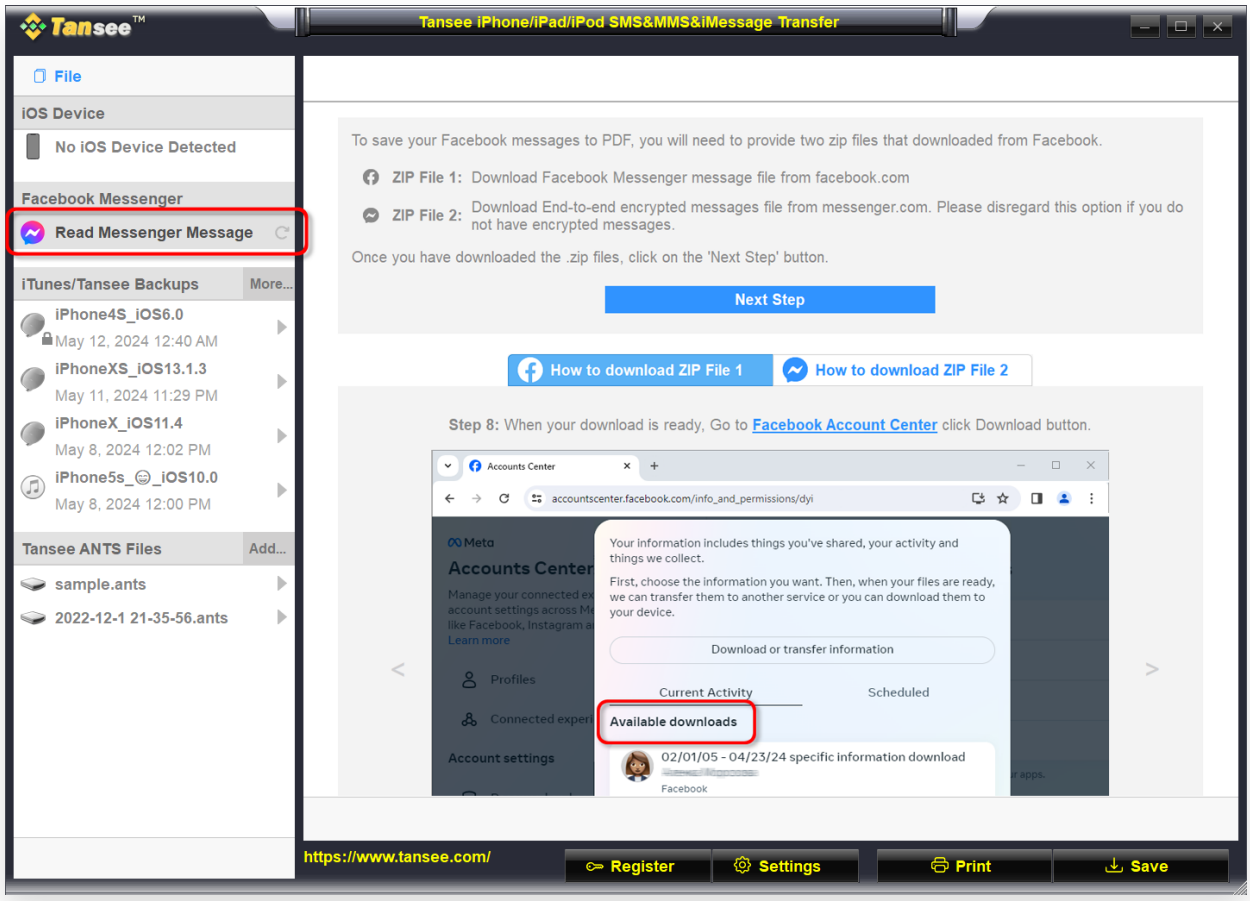
6. Fai clic su **Scarica**.

Passaggio 2: **Tansee iPhone Message Transfer o Tansee Android Message Transfer possono estrarre i file zip scaricati da Facebook.**

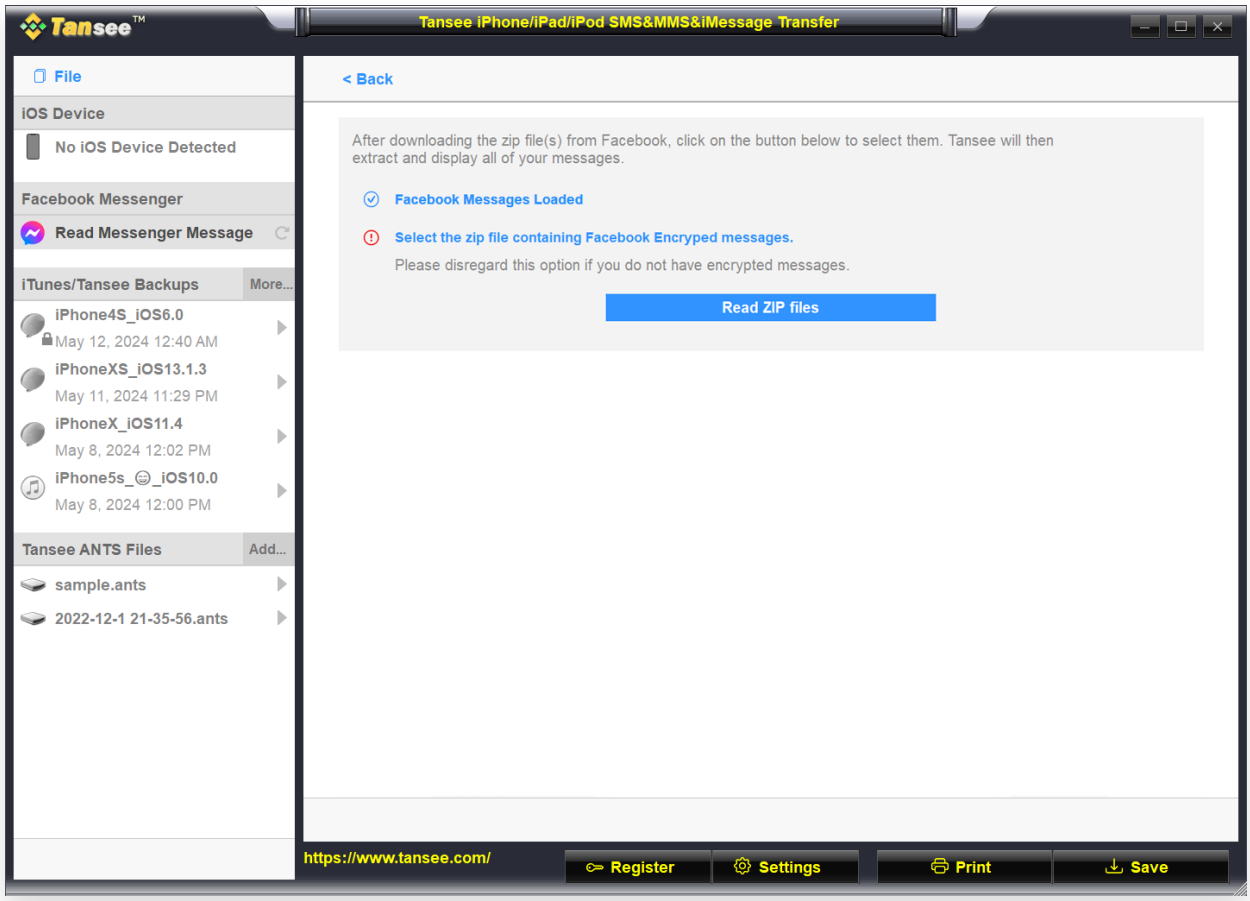
Tansee può essere utilizzato per salvare tutti i messaggi di Facebook Messenger, inclusi tutti gli allegati, come file PDF.
Dopo aver scaricato i file zip da Facebook, scarica e installa l'ultima versione di Tansee iPhone Message Transfer qui.
In alternativa, puoi scaricare e installare l'ultima versione di Tansee Android Message Transfer qui.

1. Apri Tansee iPhone Message Transfer o Tansee Android Message Transfer.
2. Fare clic sull'opzione "Leggi messaggi di Messenger".
3. Seleziona il file zip che contiene i tuoi messaggi Facebook.
4. Fai clic su "Leggi file zip" e Tansee estrarrà e visualizzerà automaticamente tutti i tuoi messaggi.

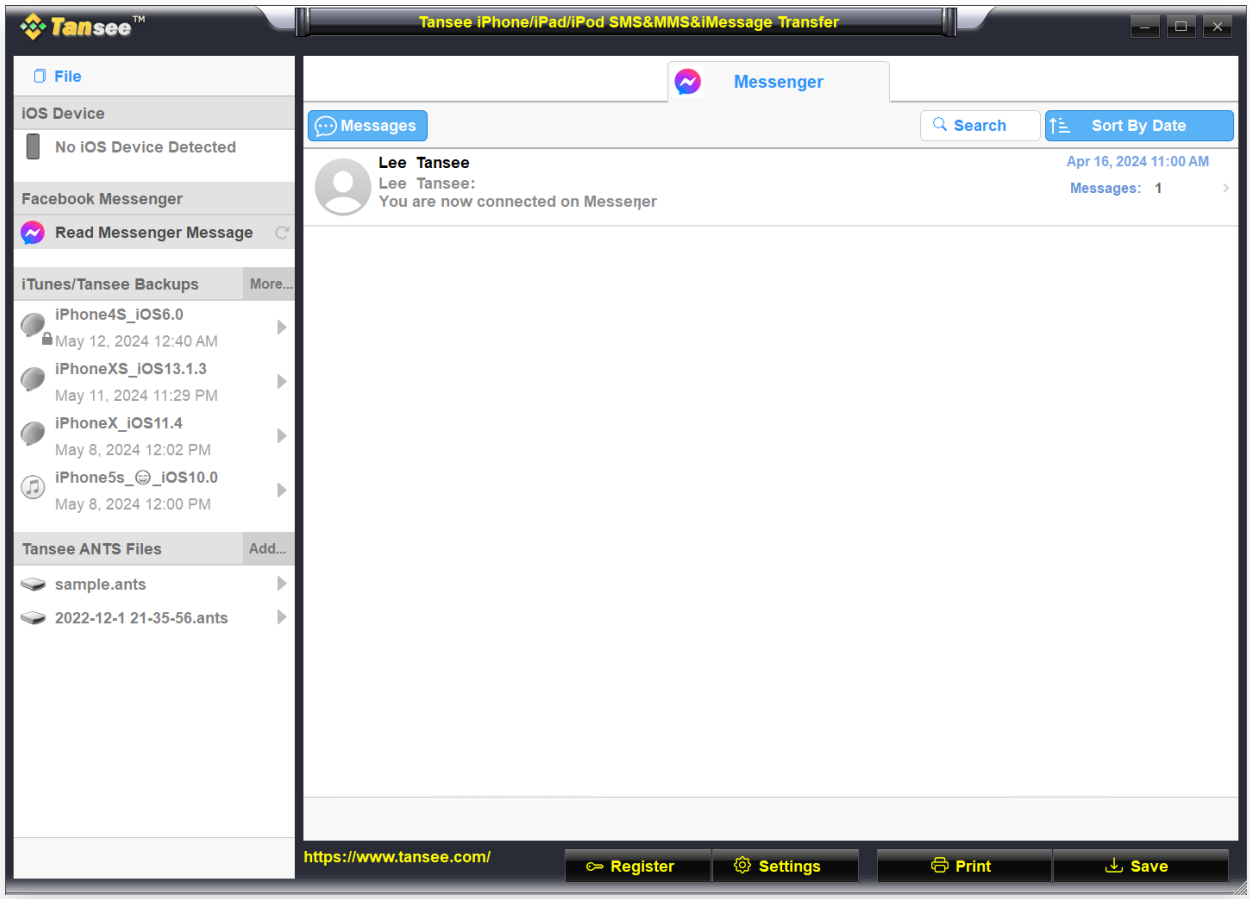
5. Una volta che Tansee ha finito di leggere tutti i tuoi messaggi, fai clic sul pulsante Salva e seleziona il formato del file PDF.



Fai clic sull'opzione "Leggi messaggi di Messenger".



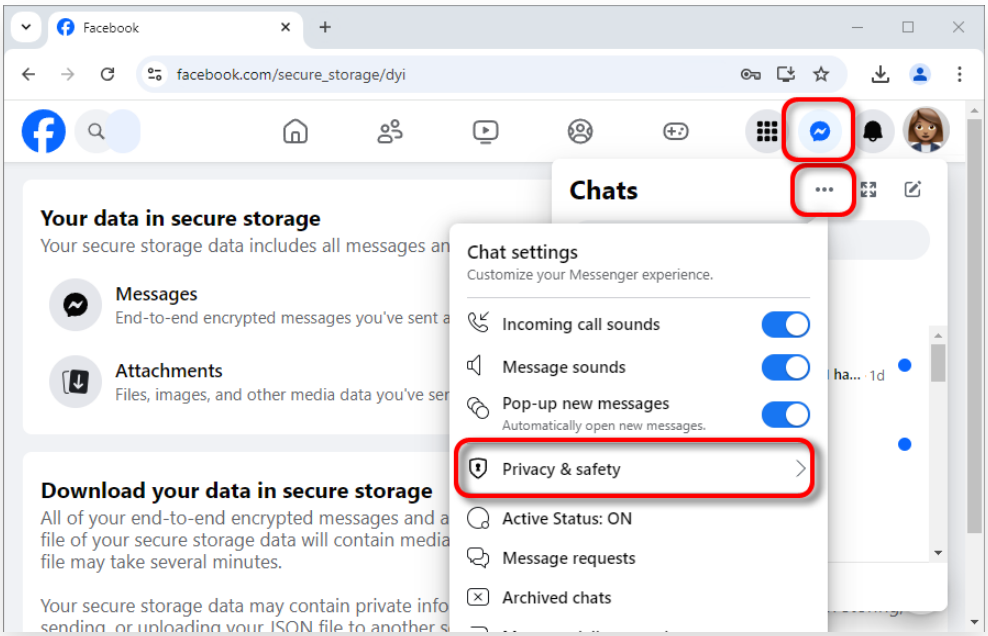
Seleziona il file zip che contiene i tuoi messaggi Facebook.



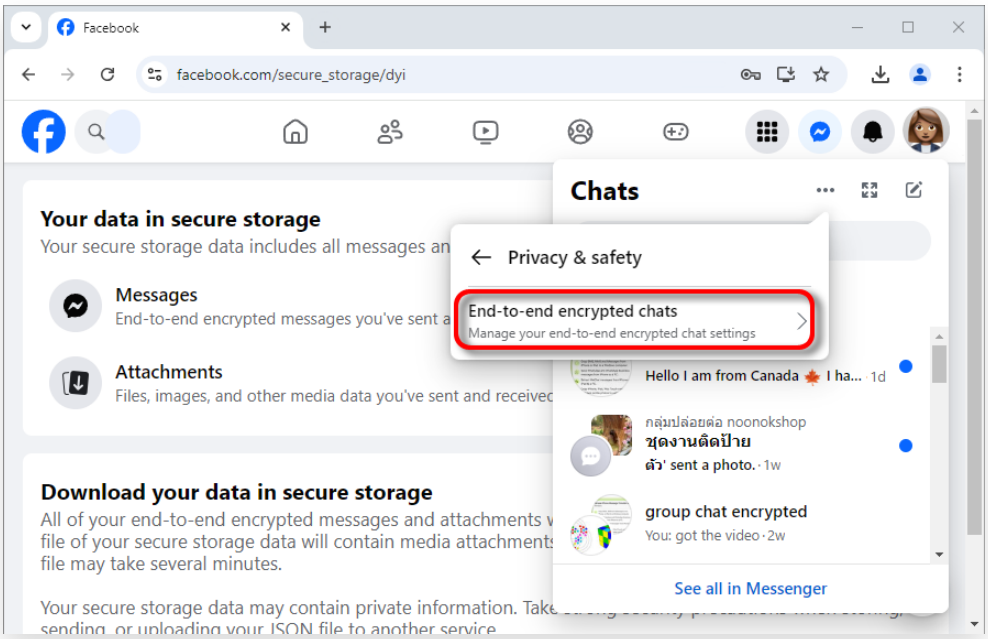
Fai clic su "Leggi file zip" e Tansee estrarrà e visualizzerà automaticamente tutti i tuoi messaggi.

Come attivare l'archiviazione sicura?

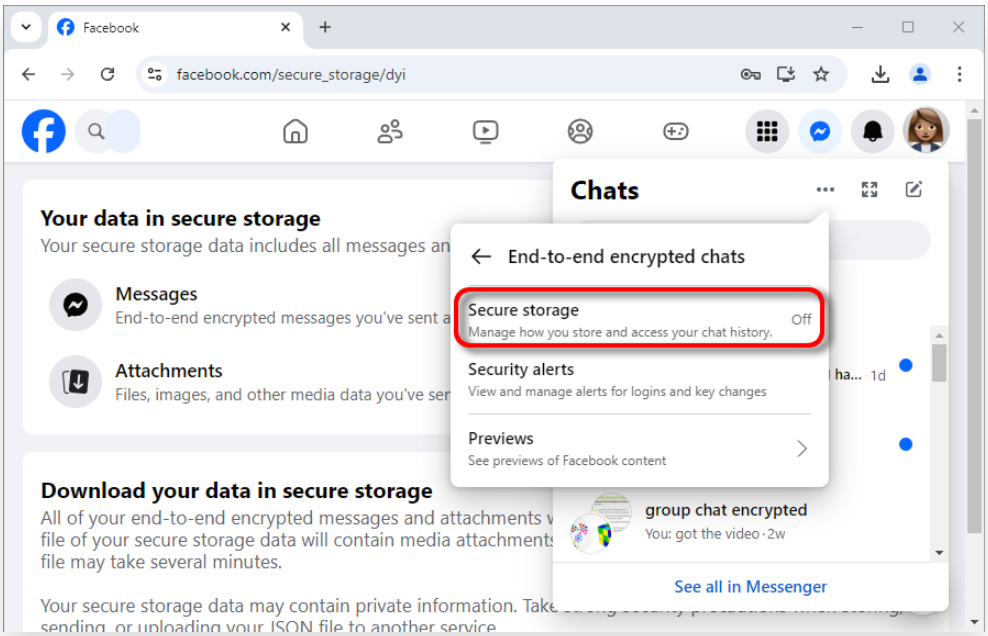
1. 1.Su un computer, apri facebook.com e accedi al tuo account. Clic . Quindi fare clic su (l'icona a tre punti) e selezionare Privacy e sicurezza.
2. Fai clic su **Chat crittografate end-to-end**.
3. Fai clic su **Archiviazione protetta**, quindi su **Attiva archiviazione protetta**.
4. **Inserisci il tuo PIN**. L'utilizzo di un account Google su dispositivi mobili Android o di un account Apple su dispositivi mobili iOS ti consentirà di accedere senza dover inserire un PIN.
5. Seguire le istruzioni visualizzate sullo schermo. Se hai creato un PIN, ricordati di conservarlo in un posto sicuro. Ne avrai bisogno per ripristinare le tue chat in un archivio sicuro su un nuovo dispositivo.



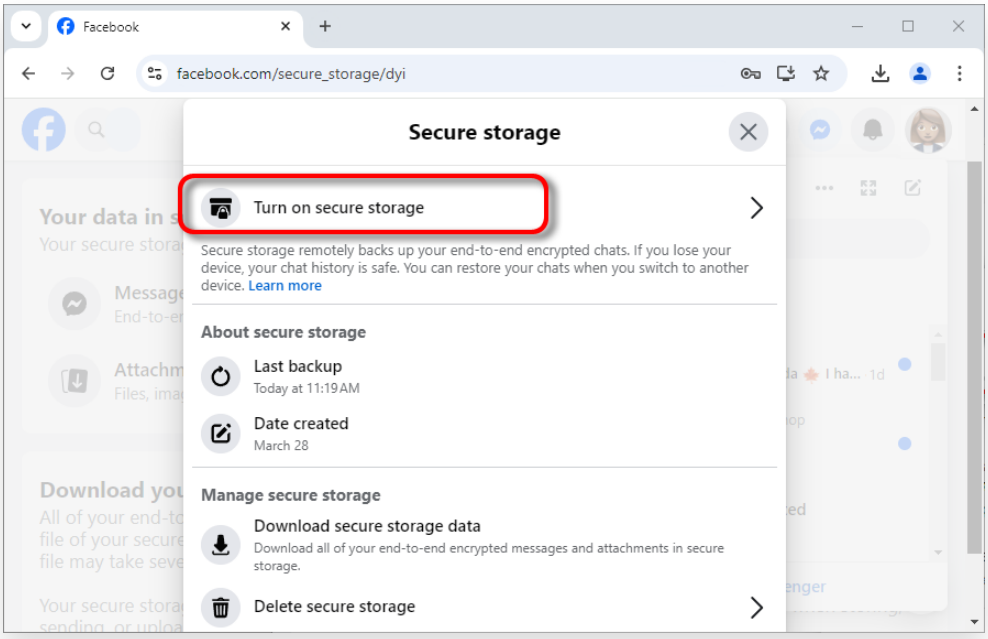
1. Clic . Quindi fare clic su (l'icona a tre punti) e selezionare Privacy e sicurezza.



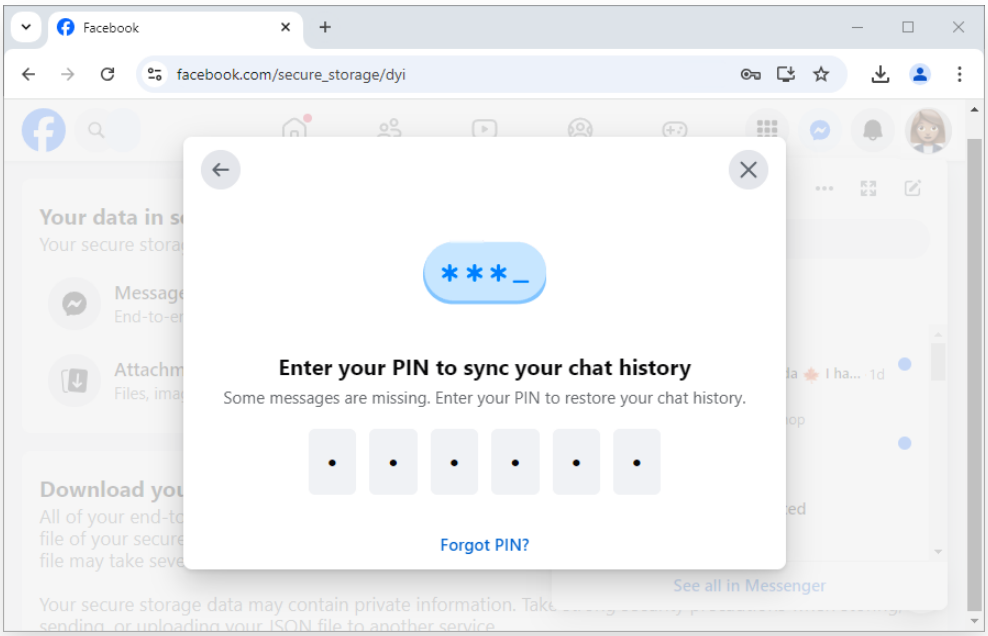
2. Fai clic su **Chat crittografate end-to-end**.



3. Fai clic su **Archiviazione sicura**.



quindi fai clic su **Attiva archiviazione sicura**.



4. Inserisci il tuo PIN.

Cosa succede se l'archiviazione sicura di Facebook è disattivata?

Quando l'archiviazione sicura di Facebook è disattivata:
Non potrai ripristinare la cronologia dei messaggi crittografati end-to-end se sostituisci il dispositivo.
Il tuo dispositivo interromperà il backup dei nuovi messaggi crittografati end-to-end.
Se scegli di eliminare l'archivio protetto:
Qualsiasi backup dei tuoi messaggi crittografati end-to-end verrà eliminato definitivamente.
I messaggi salvati sul tuo dispositivo non saranno interessati.
Nota: i nuovi messaggi crittografati end-to-end verranno archiviati solo sul tuo dispositivo, non in un archivio sicuro.
Se decidi di attivare l'archiviazione sicura in un secondo momento, tutte le tue chat crittografate end-to-end sul tuo dispositivo verranno salvate nell'archiviazione sicura. Ciò significa che se sostituisci il tuo dispositivo e utilizzi Facebook, puoi ripristinare la cronologia dei messaggi.

Cosa significa crittografia end-to-end su Messenger?

Alcuni prodotti attualmente non supportano la crittografia end-to-end, come le chat della community per i gruppi Facebook, le chat con account aziendali e professionali, le chat del Marketplace e altre.
La crittografia end-to-end su Messenger aggiunge ulteriore sicurezza e protezione ai tuoi messaggi e alle tue chiamate in modo che solo tu e la persona con cui stai parlando possiate vederli, ascoltarli o leggerli.
Il contenuto dei tuoi messaggi e delle tue chiamate nelle conversazioni

crittografate end-to-end è protetto dal momento in cui lascia il tuo dispositivo fino al momento in cui raggiunge il dispositivo del destinatario.
Ciò significa che nessun altro può vedere o ascoltare ciò che viene inviato o detto, nemmeno Meta. Non potremmo nemmeno se volessimo.

In che modo la crittografia end-to-end protegge la tua conversazione?

Ogni dispositivo in una conversazione crittografata end-to-end ha una chiave speciale per proteggere la conversazione. Quando invii un messaggio in una conversazione crittografata end-to-end, il tuo dispositivo blocca il messaggio durante l'invio. Questo messaggio può essere sbloccato solo da un dispositivo che dispone di una delle chiavi per quella conversazione.
Nessuno può accedere ai tuoi messaggi o alle tue chiamate tranne le persone con le chiavi. Tu e la persona con cui stai parlando in conversazioni crittografate end-to-end siete le uniche persone con chiavi univoche e corrispondenti.