

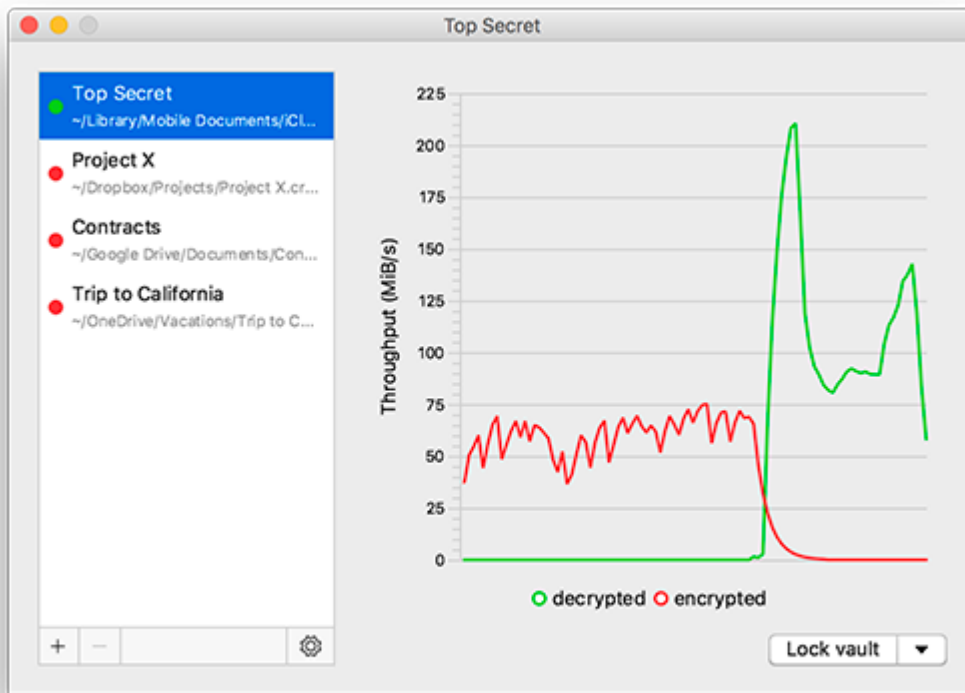
# Cryptomator

Cryptomator è un programma di crittografia gratuita lato client per i tuoi file cloud.

Software open source: nessuna backdoor, nessuna registrazione.



l'interfaccia è veramente minimale devi solo indicare la cartella dei file da crittografare ed inserire la password, l'unica cosa che vedi è il flusso dei dati durante la crittografazione, è molto veloce, puoi criptare dati su pendrive cartelle condivise su cloud, praticamente ovunque, il programma esiste per tutte le piattaforme, Linux, Mac e Windows.



<https://cryptomator.org/>

---

## Tools di recupero file

Se servono questi tools probabilmente siete stati infettati da qualche virus...

Questi tools posso aiutare a recuperare file criptati o cancellati da virus informatici, ovviamente non c'è una certezza del recupero, però conviene provarci, inoltre se i dati sono di notevole importanza, conviene rivolgersi a una agenzia specializzata...

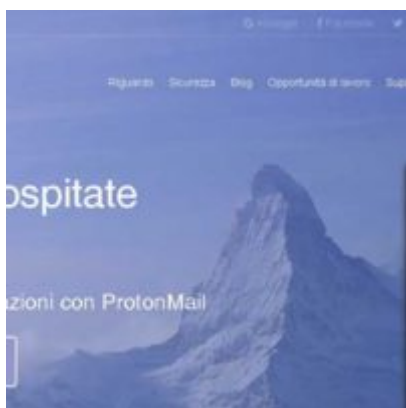
<https://support.kaspersky.com/viruses/utility>

---

# Email anonime con protonmail

Un metodo molto efficace per inviare email anonime è il servizio offerto da

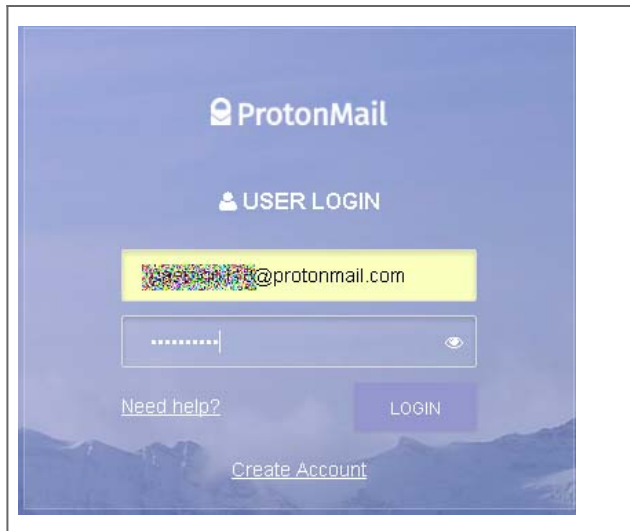
[protonmail](https://protonmail.com)



Il servizio ha due forme, una gratuita e una a pagamento, quella a pagamento offre molte più cose.

Ovviamente noi ci occupiamo solo di quella free che già è più che sufficiente per inviare email criptate di tutto rispetto.

Facciamo una registrazione scegliendo quella free, la casella sarà subito pronta a funzionare, facciamo il login mettendo tutto l'indirizzo email e la password scelta..

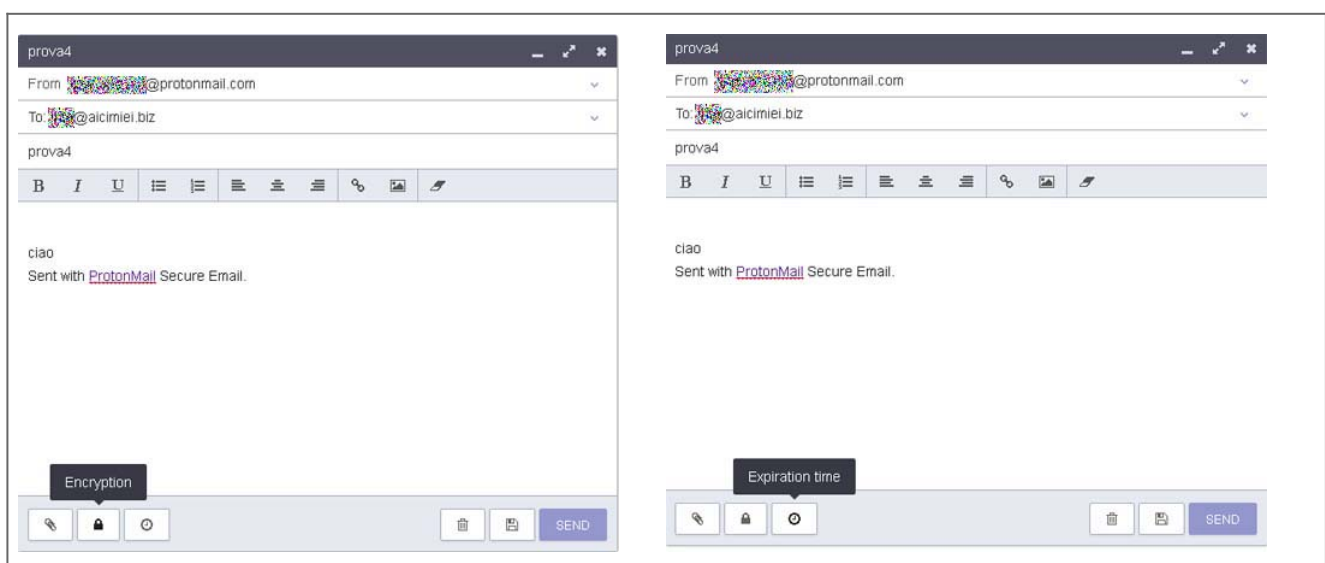


Vorrei andare al dunque per quanto riguarda l'invio di email criptate..

L'interfaccia non è in italiano ma risulta essere come qualsiasi altro servizio di posta.

Clicchiamo su "Compose" per creare un nuovo messaggio,

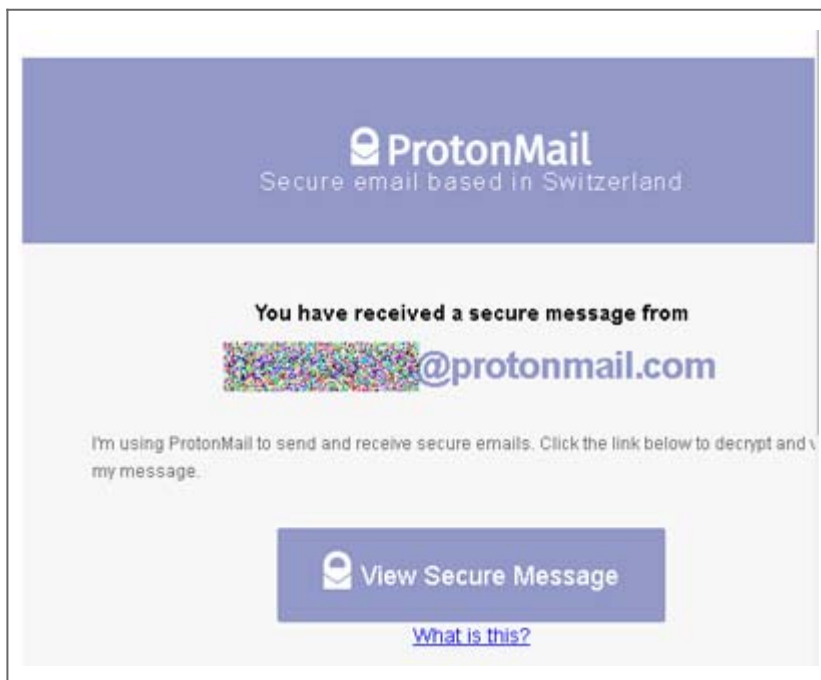
Inseriamo il destinatario, il soggetto e il testo del messaggio, se necessario aggiungere eventuali allegati. Ora in basso a destra ci sono due tasti, uno "Encryption" che serve a criptare l'email e uno "expiration Time" che imposta per quanto tempo sarà disponibile l'email prima che venga cancellata definitivamente.



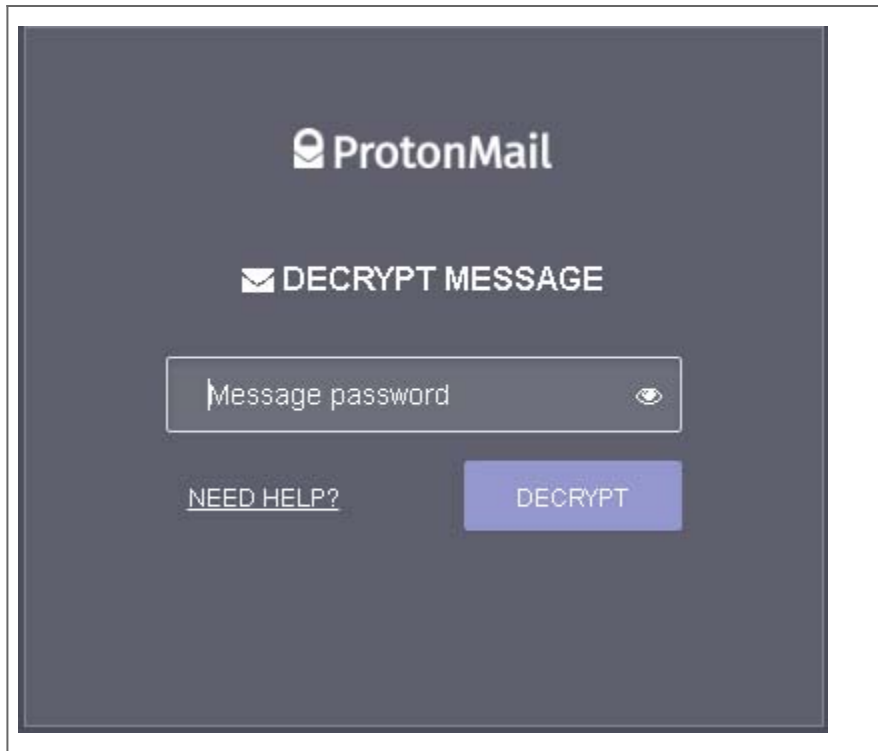
quando clicchiamo su "Encryption" ci viene chiesto di inserire una password e anche un suggerimento per la password, qualora non abbiamo contatti con l'interlocutore.

The image shows a browser window titled 'prova4' with a dialog box for encrypting messages. The dialog has the title 'Encrypt for non-ProtonMail users' with an information icon. It contains three input fields: 'Message Password' (with six dots), 'Confirm Password' (with six dots), and 'Password Hint (Optional)' (with the text '1234'). Below the fields is a note: 'Encrypted messages to non-ProtonMail recipients will expire in 28 days unless a shorter expiration time is set.' At the bottom are 'CANCEL' and 'SET' buttons.

Facciamo qualche prova per vedere il comportamento dell'email,  
Questa sarà l'email che riceviamo



Ora per leggere l'email dobbiamo cliccare sull'immagine con scritto "View Secure Message" infatti l'email vera e propria non la riceveremo mai, ma risiederà sul server.



Inseriamo la password e clicchiamo su "Decrypt" ed ecco il nostro messaggio

