

Encryptio — Manuale utente

Come usare Encryptio sul web e nell'estensione

1. Cos'è Encryptio

Encryptio è un gestore di password e note segrete. La cifratura avviene nel browser: il server conserva solo dati già chiusi e non può leggere il vault.

Disponibile come applicazione web e come estensione del browser (Chrome, Firefox, Edge): sblocchi il vault, usi Compila sulla scheda attiva oppure apri un sito dal vault per compilare. Safari usa l'app web.

2. Registrazione e accesso

Registrazione: inserisci un'email che controlli e accetta Termini e Privacy. Ricevi un link monouso (30 minuti), poi scegli la password principale (minimo 12 caratteri).

Accesso: email + password principale. Se hai attivato la 2FA, inserisci anche il codice dell'app autenticatore o un codice di backup.

Se ricarichi la pagina la sessione può restare attiva, ma il vault va sbloccato di nuovo con la password principale.

Puoi cambiare l'email dell'account in Profilo (password principale + link monouso al nuovo indirizzo). Il vault non viene toccato.

3. Password principale e sicurezza

La password principale non lascia mai il dispositivo. Encryptio non può reimpostarla né aprire i tuoi dati senza di essa.

Dal browser derivano due chiavi: una apre il vault in memoria, l'altra serve solo per dimostrare l'accesso al server.

Dopo un periodo di inattività (predefinito 15 minuti, modificabile in Profilo) il vault si blocca da solo: la chiave esce dalla memoria e serve di nuovo la password principale. Restare connessi non basta.

4. Vault: password e note

Nel Vault trovi le password (titolo, utente, password, sito, tag) e le note segrete (testo lungo).

Puoi cercare, paginare e importare/esportare JSON o CSV in chiaro sul tuo computer. Non esiste un export lato server: i download restano sul dispositivo.

Il file di export contiene le tue password in chiaro: conservalo in un posto sicuro ed eliminalo dopo l'uso.

Con l'estensione Encryptio installata, un clic sull'URL di una password apre il sito e compila i campi di login. Senza estensione il link si apre comunque.

Piano Starter: fino a 15 password e 15 note. Premium toglie quei limiti.

5. Kit di recupero

In Profilo → Sicurezza puoi creare un kit di recupero: una chiave di recupero da conservare offline, che permette di riaprire i tuoi dati se dimentichi la password principale.

Per usarla: vai su "Password dimenticata", apri il link che ricevi via email (valido 24 ore) e inserisci la chiave

di recupero.

Senza kit, se perdi la password principale i dati restano cifrati per sempre, anche per noi.

6. Autenticazione a due fattori (2FA)

Opzionale. Protegge solo l'accesso all'account, non sostituisce la password principale per sbloccare il vault.

Attivala in Profilo, scansiona il QR o inserisci il secret nell'app autenticatore, poi conserva i codici di backup monouso.

7. Digital Legacy

In Profilo → Digital Legacy (Premium) puoi nominare fino a cinque contatti di fiducia, in ordine di priorità.

Quando aggiungi un contatto, il browser crea una chiave di accesso Legacy e un wrap della vault key. La chiave viene mostrata una sola volta: consegnala al contatto fuori banda (stampa o canale sicuro). Non arriva via email da Encryptio.

Il contatto può richiedere l'accesso dalla pagina pubblica `/legacy/request`. Parte un periodo di attesa (configurabile); puoi annullare in qualsiasi momento da Profilo.

Dopo il grant riceve un link: deve confermare (protezione da prefetch delle email) e inserire la chiave Legacy. Apre una vista in sola lettura, a tempo: niente modifiche, export o condivisioni.

Con più contatti, se la finestra scade senza che il delegato apra l'accesso, il sistema passa al contatto successivo (escalation).

Opzionale: trigger di inattività. Dopo i giorni impostati ricevi un avviso in grazia; se non accedi, il contatto prioritario può ricevere il grant. Resta zero-knowledge: Encryptio non tiene mai la vault key in chiaro né in escrow.

Se cambi la password principale o recuperi il vault con il kit, i contatti Legacy vengono azzerati: dovrai riaggiungerli e consegnare nuove chiavi.

Senza Premium (o prova attiva) non puoi configurare Digital Legacy; le richieste dei contatti non partono.

8. Piani e prezzi

Starter: gratuito. Premium: 3,99 €/mese oppure 2,79 €/mese con fatturazione annuale. Prova Premium di 30 giorni (una sola volta, senza carta).

Premium toglie i limiti di voci e aggiunge la condivisione monouso sicura e Digital Legacy.

Se torni da Premium a Starter con più di 15 voci per tipo, le 15 più vecchie restano modificabili; quelle in eccesso sono solo lettura ed eliminazione finché non riduci l'elenco o torni a Premium. Puoi comunque esportare tutto.

L'abbonamento a pagamento passa da PayPal (checkout lato server). Dettagli sulla pagina Prezzi del sito.

9. Estensione del browser

Chrome, Firefox ed Edge: installa il pacchetto nuovo (non l'estensione del vecchio Encryptio). Imposta l'URL API in Opzioni se serve.

Dal popup: sblocca con la password principale (e 2FA se attiva), cerca, Compila sulla scheda aperta oppure Apri per andare al sito e compilare.

Dal vault web, con l'estensione attiva, il clic sull'URL della password apre e compila. La chiave resta in memoria nell'estensione e si blocca dopo circa 15 minuti di inattività.

10. Generatore e strumenti

Il Generatore crea password casuali o frasi memorabili (IT/EN) nel browser. Nulla viene inviato al server.

Cifra testo (/tools/cipher) sigilla un testo con una password scelta da te, sempre nel browser. Non è collegato al vault né al kit di recupero.

11. Assistenza

FAQ, Novità e Contatti sono nel menu Supporto del sito. Il manuale PDF è nello stesso menu. Come funziona spiega anche Digital Legacy. Non incollare password o contenuti del vault nei messaggi di contatto o nei suggerimenti.