

Encryptio — User manual

How to use Encryptio on the web and in the extension

1. What Encryptio is

Encryptio is a password and secret-note manager. Encryption happens in the browser: the server stores already-locked data only and cannot read your vault.

Available as a web app and a browser extension (Chrome, Firefox, Edge): unlock the vault, use Fill on the active tab, or open a site from the vault to autofill. Safari uses the web app.

2. Registration and sign-in

Registration: enter an email you control and accept Terms and Privacy. You get a one-time link (30 minutes), then choose a master password (at least 12 characters).

Sign-in: email + master password. If 2FA is on, also enter an authenticator or backup code.

After a page refresh the session may remain, but you must unlock the vault again with the master password.

You can change the account email in Profile (master password + one-time link to the new address). The vault is not touched.

3. Master password and security

The master password never leaves your device. Encryptio cannot reset it or open your data without it.

The browser derives two keys: one opens the vault in memory; the other only proves sign-in to the server.

After inactivity (default 15 minutes, changeable in Profile) the vault locks by itself: the key leaves memory and you must enter the master password again. Staying signed in is not enough.

4. Vault: passwords and notes

The Vault holds passwords (title, username, password, site, tags) and secret notes (long text).

You can search, paginate, and import/export plaintext JSON or CSV on your computer. There is no server-side export: downloads stay on your device.

The export file contains your passwords in the clear: keep it somewhere safe and delete it after use.

With the Encryptio extension installed, clicking a password URL opens the site and fills the login fields. Without the extension the link still opens.

Starter plan: up to 15 passwords and 15 notes. Premium removes those limits.

5. Recovery kit

In Profile → Security you can create a recovery kit: a recovery key to keep offline, so you can reopen your data if you forget the master password.

To use it: go to Forgot password, open the email link you receive (valid 24 hours), and enter the recovery key.

Without a kit, if you lose the master password the data stays encrypted forever — including for us.

6. Two-factor authentication (2FA)

Optional. It protects account sign-in only and does not replace the master password for vault unlock.

Enable it in Profile, scan the QR or enter the secret in an authenticator app, then store the one-time backup codes.

7. Digital Legacy

In Profile → Digital Legacy (Premium) you can name up to five trusted contacts, ordered by priority.

When you add a contact, the browser creates a Legacy access key and a wrap of the vault key. The key is shown once: give it to the contact out of band (print or a secure channel). Encryptio does not email it.

The contact can request access from the public page `/legacy/request`. A waiting period starts (configurable); you can cancel anytime from Profile.

After grant they get a link: they must confirm (anti-prefetch) and enter the Legacy key. They open a timed read-only view — no edits, export, or shares.

With multiple contacts, if the window expires without the delegate opening access, the system moves to the next contact (escalation).

Optional: inactivity trigger. After the set idle days you get a grace warning; if you don't sign in, the top-priority contact may receive the grant. Still zero-knowledge: Encryptio never holds the vault key in the clear or in escrow.

If you change the master password or recover the vault with the kit, Legacy contacts are cleared: re-add them and hand out new keys.

Without Premium (or an active trial) you cannot configure Digital Legacy; contact requests will not start.

8. Plans and pricing

Starter: free. Premium: €3.99/month or €2.79/month billed yearly. One-time 30-day Premium trial (no card).

Premium removes item limits and adds one-time secure share and Digital Legacy.

If you return from Premium to Starter with more than 15 items per type, the oldest 15 stay editable; newer excess items are view and delete only until you trim the list or go Premium again. You can still export everything.

Paid subscriptions use PayPal (server-side checkout). See the Pricing page on the site.

9. Browser extension

Chrome, Firefox, and Edge: install the new package (not the old Encryptio extension). Set the API URL in Options if needed.

From the popup: unlock with the master password (and 2FA if enabled), search, Fill on the open tab, or Open to go to the site and fill.

From the web vault, with the extension active, clicking the password URL opens and fills. The key stays in extension memory and locks after about 15 minutes of inactivity.

10. Generator and tools

The Generator builds random passwords or memorable passphrases (IT/EN) in the browser. Nothing is sent to the server.

Encrypt text (/tools/cipher) seals text with a password you choose, always in the browser. It is not linked to the vault or the recovery kit.

11. Support

FAQ, What's new, and Contact are under Support in the site menu. The PDF manual is in the same menu. How it works also covers Digital Legacy. Never paste passwords or vault contents into contact messages or product suggestions.