

Step 1 of 2

## Sign in or join.

1

We send a one-time code to your email. No password; if you have no account yet, it is created when the code is verified.

2

Email

you@example.com

3



Doğrulaniyor...



Send code

4

Your address is never shown publicly; only its digest is stored. Comments show your handle.

# How the CSINT Community is built

The CSINT Community is the site's membership area. You sign in with a one-time code sent to your email, choose a handle and can leave comments under articles. This handbook explains how I built it without a password database and what is stored.

## 1 Why there is no password

A password database is one of the most harmful things to leak. People reuse the same password elsewhere. A small research site does not need to carry that risk. So I tied sign-in to a one-time code sent by email.

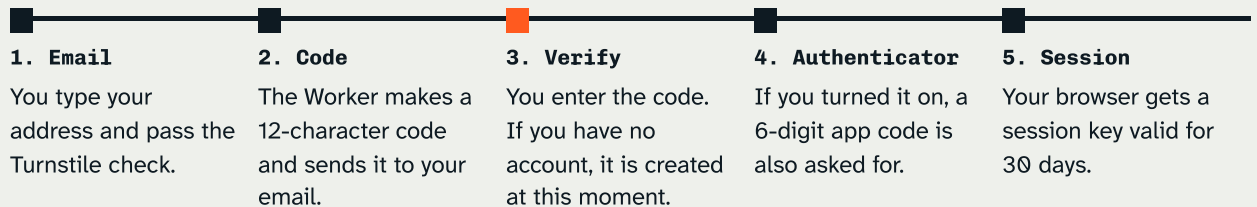
The site is a static export. Membership, comments and moderation run in a separate Cloudflare Worker. The Worker keeps its data in a Cloudflare D1 database.

### A few words

|                             |                                                                                                                             |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>One-time code</b>        | A code sent to your email that is valid for 10 minutes and can be used only once.                                           |
| <b>Digest (hash)</b>        | A fingerprint computed from a value that cannot be turned back. The Worker keeps the digest of your email, not the address. |
| <b>Session key</b>          | A random key given to your browser after sign-in. The server keeps only its digest.                                         |
| <b>Authenticator (TOTP)</b> | The 6-digit code from the authenticator app on your phone, which changes every 30 seconds.                                  |
| <b>Turnstile</b>            | Cloudflare's check that the person filling in a form is human.                                                              |

---

## 2 How sign-in works



Step 1 of 2

## Sign in or join.

- 1 We send a one-time code to your email. No password; if you have no account yet, it is created when the code is verified.
- 2 Email  
you@example.com
- 3    
**Send code**
- 4 Your address is never shown publicly; only its digest is stored. Comments show your handle.

The sign-in card on the live community page. The email field is empty. The human check was still running when I took this screen. I did not request a code or try to pass verification.

**1 No password**

The card says it first. There is no separate sign-up; the account is created after the first correct code.

**2 Email**

To send the code, the address is handed to the email delivery service at that moment. The database stores its SHA-256 digest, not the address.

**3 Human check**

No code can be requested before the Turnstile check passes. This cuts down automated code requests and email flooding.

**4 Shown name**

Your address never appears on a public profile. Comments show only your handle.

---

### 3 Rules for codes and sessions

|                          |                                                                                                                                           |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Code</b>              | 12 characters, valid 10 minutes, at most 3 attempts. A correct code is marked used in a single operation and will not work a second time. |
| <b>Wrong address</b>     | An invalid address gets the same answer. So from outside you cannot tell whether an address is registered.                                |
| <b>Session</b>           | A random key. The server keeps only its digest. Valid for at most 30 days.                                                                |
| <b>Cookie</b>            | HttpOnly and Secure. The page's JavaScript cannot read it, and it is only sent over an encrypted connection.                              |
| <b>Origin check</b>      | Every request that changes something must come from an allowed site. A form sent from another site is refused.                            |
| <b>Authenticator</b>     | Optional. The secret key sits encrypted in the database. 8 recovery codes are given, and only their digests are kept.                     |
| <b>Rate limits</b>       |                                                                                                                                           |
| <b>Requesting a code</b> | 3 per 15 minutes per address, 10 per hour per IP.                                                                                         |
| <b>Entering a code</b>   | 6 attempts per 15 minutes.                                                                                                                |
| <b>Comments</b>          | 20 per hour.                                                                                                                              |
| <b>Reports</b>           | 10 per day.                                                                                                                               |
| <b>Changing handle</b>   | 2 per day.                                                                                                                                |

---

### 4 What is stored, what is not

|                               |                                                                     |
|-------------------------------|---------------------------------------------------------------------|
| <b>Email address</b>          | Only its SHA-256 digest. The plain address is not kept.             |
| <b>Password</b>               | None. It is never asked for.                                        |
| <b>Session</b>                | Only the digest of the key.                                         |
| <b>IP and browser details</b> | Only as digests.                                                    |
| <b>Account</b>                | Handle, role and account state.                                     |
| <b>Community records</b>      | Comments, reactions, reports, moderation records and notifications. |
| <b>Medium articles</b>        | Not copied. Only the latest article list is cached.                 |

## For how long

**Used or expired codes** Deleted 24 hours after they expire.

**Closed sessions** Deleted 7 days after they end or are revoked.

**Rate limit records** 7 days.

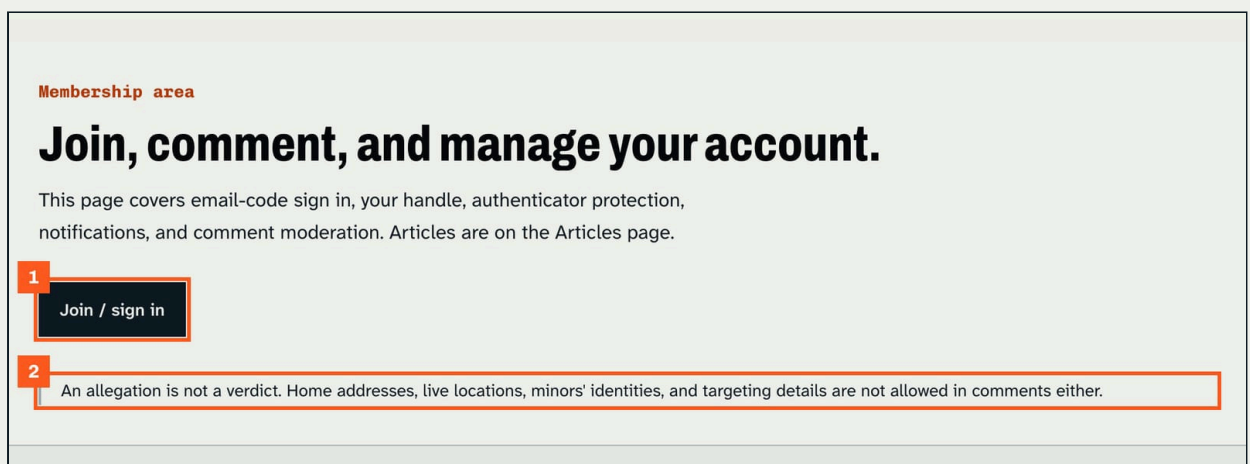
**Notifications** 90 days.

The Worker does this cleanup by itself every day. A separate timer is set up for it.

---

## 5 Moderation

- 1 Comments are 2 to 2000 characters. Comments are written on the article pages, not on this page.
- 2 Before publishing, the Worker checks a comment for patterns for selling substances, instructions for using them, self-harm instructions and personal data (phone, national ID, IBAN, home address). A comment that matches is not deleted, it waits for human review.
- 3 A moderator can publish, hide or delete a comment, and can mute a member for a set time or ban them. Every moderation action is recorded.
- 4 The admin role comes only from an email list in the Worker settings. Nobody can give themselves admin rights from the interface.



The top of the community page, when not signed in.

- 1 **Join or sign in**  
Opens the sign-in card. Once signed in, your handle and the account and security, notifications and sign-out buttons appear here.
- 2 **Comment rule**  
An allegation is not a verdict. Home addresses, live locations, minors' identities and targeting details are not allowed in comments either.

---

## 6 What it does not do

- ✗ Passwordless sign-in does not remove every risk. Someone who takes over your email account can also reach the code. That is why I suggest turning on Authenticator protection.
- ✗ Comments are not verified information by themselves. A claim in the community is not a verdict.
- ✗ The page is closed to search engines. The community page is for managing your account, not a showcase.

In short, your email works like a key but is not kept. The server knows you only by the digest of your address.