

Cookies and fingerprints

How websites recognize you, and what you can do

THE QUESTION

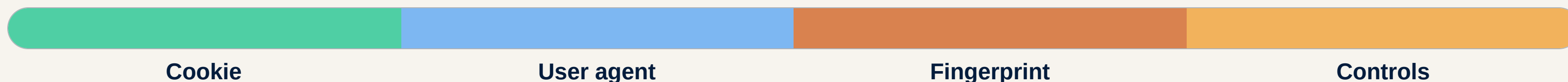
How does a website know it is you, even after you leave and come back?

THE PROMISE

You will see a real cookie, your own user agent and your own fingerprint.

OUR JOB

Learn what each one reveals, and which controls really help.



What a cookie is

```
1 Browser asks for a page
2 Server replies:
  Set-Cookie: id=abc123; Max-Age=86400; Secure
3 Browser stores the cookie
4 Every later request carries it:
  Cookie: id=abc123
```

- A cookie is only text. It cannot run code.
- Many are useful: sign-in, cart, language
- First party: set by the site you visit
- Third party: set by an outside company on that page
- Session cookies end when you close the browser. Others last until a date.

WHAT IT HOLDS

name=value

Domain

Path

Max-Age

Secure

HttpOnly

SameSite

The harm is not the cookie. It is a unique ID that follows you.

How cookies become **tracking**

recipes.example

loads ad.example

Cookie: id=abc123

news.example

loads ad.example

Cookie: id=abc123

shop.example

loads ad.example

Cookie: id=abc123

↓ **same ID on every site** ↓

ad.example: Visitor abc123 read recipes, local news and hiking boots

- A third party sees you on many sites and links the visits
- Companies swap IDs to match profiles (cookie syncing)
- Browsers differ: some block or separate third-party cookies by default

Deleting cookies resets the ID. Does that stop a tracker from recognizing you?

What to watch for **in the demo**

Your cookie

- A real cookie, set in your browser
- What it stores, and for how long
- What your browser sends back
- How a tracker can follow one across sites

Your user agent and fingerprint

- What your browser tells every site
- Details that combine into an ID
- What happens to the ID when you delete cookies
- How narrowing a crowd works

Predict: if you delete all your cookies, can a website still recognize your browser?

Write yes or no, and why. We'll test it in the lab.