

## FLASH CARDS

# Cookies and fingerprints

Terminology and quiz cards for the Take Back Your Bytes lesson on cookies, user agents and browser fingerprinting.

## What is in this set

---

40 cards: **24 term cards** (term on the front, definition on the back) and **16 quiz cards** (question on the front, answer on the back). Bracketed numbers on the backs, like [1], match the reference list on the last page and in the instructor guide.

## How to print

---

1. Print double-sided on US Letter at 100% scale (no "fit to page").
2. Choose **flip on the long edge**. The backs are arranged so each answer lands behind its card.
3. Cut along the dashed lines. Each card is 3.75 by 2.5 inches.

## How to use them

---

- **Self-test:** read the front, answer aloud, flip to check.
- **Pairs:** one reads the front, the other answers. Swap every five cards.
- **Boxes:** keep a "missed" pile and a "got it" pile. Re-test the missed pile after a break, then again the next day.
- **Warm-up:** deal a few quiz cards at the start of the next session.

Facts checked October 27, 2026. Tools and models change quickly, so confirm details against the current documentation. These materials are dedicated to the public domain under CC0 1.0 and shared for the public good. The PrivacySafe and PrivacySafe Foundation names and logos are trademarks and are not included in that dedication.

TERM

1 / 40

# Cookie

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

2 / 40

# Set-Cookie

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

3 / 40

# Cookie header

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

4 / 40

# Session cookie

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

5 / 40

# Persistent cookie

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

6 / 40

# Max-Age

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

7 / 40

# Secure

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

8 / 40

# HttpOnly

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

2 / 40

The response header a server uses to ask the browser to store a cookie.

[\[2\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

1 / 40

A small piece of text a site asks your browser to keep and send back on later requests.

[\[1\]](#) [\[3\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

4 / 40

A cookie with no set lifetime. It normally ends when the browser session ends.

[\[1\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

3 / 40

The request header the browser uses to send stored cookies back to the site.

[\[1\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

6 / 40

A cookie setting for how many seconds it lasts. Zero or less expires it at once.

[\[2\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

5 / 40

A cookie with a Max-Age or Expires, so it lasts until a time or date.

[\[1\]](#) [\[2\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

8 / 40

A cookie setting that hides the cookie from page scripts. Only a server can set it.

[\[1\]](#) [\[2\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

7 / 40

A cookie setting that sends the cookie only over HTTPS.

[\[2\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

9 / 40

## SameSite

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

10 / 40

## First-party cookie

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

11 / 40

## Third-party cookie

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

12 / 40

## Cookie syncing

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

13 / 40

## Partitioned cookies

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

14 / 40

## User agent

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

15 / 40

## User-Agent string

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

16 / 40

## Mozilla/5.0

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

10 / 40

A cookie set by the site you chose to visit.

[\[4\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

9 / 40

A cookie setting for whether it is sent on cross-site requests: Lax, Strict or None.

[\[2\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

12 / 40

Companies swapping IDs to match their cookies and profiles for the same person.

[General](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

11 / 40

A cookie set by an outside company on a page you visit, which can recognize you across sites.

[\[4\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

14 / 40

The software that acts for you on the web. Usually your browser.

[\[8\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

13 / 40

Cookies kept in a separate jar for each top-level site, so a third party cannot link them across sites.

[\[2\]](#) [\[6\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

16 / 40

A historical token almost every browser still sends at the start of its user agent string.

[\[8\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

15 / 40

Text your browser sends with every request, naming its browser, version, engine and operating system.

[\[8\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

17 / 40

## User-Agent reduction

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

18 / 40

## Client Hints

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

19 / 40

## Browser fingerprint

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

20 / 40

## Canvas fingerprinting

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

21 / 40

## Anonymity set

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

22 / 40

## Cookie banner

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

23 / 40

## Global Privacy Control

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

TERM

24 / 40

## Cover Your Tracks

Say it in your own words, then flip.

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

18 / 40

A way for sites to request more detail about the browser, beyond the reduced user agent.

[\[9\]](#) [\[10\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

17 / 40

Browsers hiding the exact OS version, device model and minor version in the user agent.

[\[9\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

20 / 40

Drawing a hidden image and reading it back, because small differences by graphics stack help tell browsers apart.

[\[13\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

19 / 40

An ID made by combining many small details about your browser and device. It needs no cookie.

[\[11\]](#) [\[13\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

22 / 40

A pop-up asking you to accept or reject cookies. In the EU, pre-ticked boxes are not valid consent.

[\[16\]](#) [\[17\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

21 / 40

The group of visitors who look identical to a tracker. The smaller it is, the easier you are to pick out.

[\[11\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

24 / 40

An EFF tool that tests how well your browser resists tracking and fingerprinting.

[\[14\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**TERM**

23 / 40

A browser signal that asks sites not to sell or share your data. Some laws require honoring it.

[\[18\]](#) [\[19\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

QUIZ

25 / 40

**What is a cookie?**

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

QUIZ

26 / 40

**What turns a cookie into a tracker?**

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

QUIZ

27 / 40

**Name three settings on a cookie.**

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

QUIZ

28 / 40

**What does HttpOnly do?**

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

QUIZ

29 / 40

**How do you delete a cookie?**

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

QUIZ

30 / 40

**Why can three sites with one ad company be linked?**

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

QUIZ

31 / 40

**What does a partitioned cookie jar change?**

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

QUIZ

32 / 40

**If you delete all cookies, can a site still recognize you?**

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**QUIZ**

26 / 40

A unique ID, usually set by an outside company that appears on many sites.

[\[4\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**QUIZ**

25 / 40

A small piece of text a site asks your browser to keep and send back. It cannot run code.

[\[1\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**QUIZ**

28 / 40

It hides the cookie from page scripts. Only a server can set it.

[\[1\]](#) [\[2\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**QUIZ**

27 / 40

For example: Max-Age or Expires, Secure, HttpOnly, SameSite, Domain and Path.

[\[2\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**QUIZ**

30 / 40

The same third-party cookie ID is sent from every site, so the company joins the visits.

[\[4\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**QUIZ**

29 / 40

Set it again with the same name and scope and a Max-Age of zero.

[\[2\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**QUIZ**

32 / 40

Yes. A fingerprint, an IP address or an account can still link you.

[\[11\]](#) [\[12\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**QUIZ**

31 / 40

The same company gets a different cookie on each site, so it cannot match them.

[\[2\]](#) [\[6\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

QUIZ

33 / 40

**What does a user agent string contain?**

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

QUIZ

34 / 40

**What does User-Agent reduction hide?**

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

QUIZ

35 / 40

**What did the 2010 Panopticlick study find?**

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

QUIZ

36 / 40

**Why can a random fake value make you stand out?**

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

QUIZ

37 / 40

**Name two ways to resist fingerprinting.**

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

QUIZ

38 / 40

**In the EU, is a pre-ticked cookie box valid consent?**

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

QUIZ

39 / 40

**What does the Global Privacy Control do?**

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

QUIZ

40 / 40

**Name one step from the cookie plan.**

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**QUIZ**

34 / 40

The exact OS version, the device model and the minor browser version.

[\[9\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**QUIZ**

33 / 40

Browser, version, engine and operating system, plus the historical Mozilla/5.0.

[\[8\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**QUIZ**

36 / 40

Few other browsers would show it, so it can make your fingerprint more unusual.

[\[13\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**QUIZ**

35 / 40

83.6% of 470,161 browsers had a unique fingerprint in the sample. It is historical.

[\[11\]](#) [\[12\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**QUIZ**

38 / 40

No. The court and data protection authorities say it is not.

[\[16\]](#) [\[17\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**QUIZ**

37 / 40

For example: common settings, an updated browser, built-in protection, and few unusual add-ons.

[\[13\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**QUIZ**

40 / 40

For example: check third-party cookie settings, choose Reject on banners, test your fingerprint, use separate profiles.

[General](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

**QUIZ**

39 / 40

It sends a signal asking sites not to sell or share your data. It asks, it does not block.

[\[18\]](#) [\[19\]](#)

Cookies and fingerprints

PrivacySafe Foundation | CC0 1.0

## Reference list

Links were checked on October 27, 2026.

| #    | SOURCE                                                                                                                                                                                                                                                                                                                               | WHAT IT SUPPORTS                                                                                                                                       |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| [1]  | MDN Web Docs, Using HTTP cookies<br><a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/Cookies">https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/Cookies</a>                                                                                                                                                  | How cookies move between browser and server, session and persistent cookies, and the Secure, HttpOnly and SameSite attributes.                         |
| [2]  | MDN Web Docs, Set-Cookie header<br><a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie</a>                                                                                                                                           | Cookie attributes including Max-Age, Path, Secure, HttpOnly, SameSite and Partitioned, and deleting a cookie by expiring it.                           |
| [3]  | IETF, RFC 6265: HTTP State Management Mechanism<br><a href="https://www.rfc-editor.org/rfc/rfc6265">https://www.rfc-editor.org/rfc/rfc6265</a>                                                                                                                                                                                       | The standard that defines cookies.                                                                                                                     |
| [4]  | MDN Web Docs, Third-party cookies<br><a href="https://developer.mozilla.org/en-US/docs/Web/Privacy/Third-party_cookies">https://developer.mozilla.org/en-US/docs/Web/Privacy/Third-party_cookies</a>                                                                                                                                 | How third-party cookies enable cross-site tracking, and how browsers respond.                                                                          |
| [5]  | WebKit, Full Third-Party Cookie Blocking and More<br><a href="https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/">https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/</a>                                                                                                                 | Safari's default blocking of third-party cookies.                                                                                                      |
| [6]  | Mozilla Support, Third-party cookies and Firefox tracking protection<br><a href="https://support.mozilla.org/en-US/kb/third-party-cookies-firefox-tracking-protection">https://support.mozilla.org/en-US/kb/third-party-cookies-firefox-tracking-protection</a>                                                                      | Firefox's default protection against cross-site tracking cookies.                                                                                      |
| [7]  | Google Chrome Help, Manage cookies in Chrome<br><a href="https://support.google.com/chrome/answer/95647">https://support.google.com/chrome/answer/95647</a>                                                                                                                                                                          | Chrome's cookie settings, including the option to allow or block third-party cookies.                                                                  |
| [8]  | MDN Web Docs, User-Agent header<br><a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/User-Agent">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/User-Agent</a>                                                                                                                                           | The format of the User-Agent header and the historical Mozilla/5.0 token.                                                                              |
| [9]  | MDN Web Docs, User-Agent reduction<br><a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/User-agent_reduction">https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/User-agent_reduction</a>                                                                                                                      | What reduction removes (exact OS version, device model, minor browser version) and why the string can be used for fingerprinting.                      |
| [10] | MDN Web Docs, User-Agent Client Hints API<br><a href="https://developer.mozilla.org/en-US/docs/Web/API/User-Agent_Client_Hints_API">https://developer.mozilla.org/en-US/docs/Web/API/User-Agent_Client_Hints_API</a>                                                                                                                 | The navigator.userAgentData interface and low-entropy versus high-entropy values.                                                                      |
| [11] | Peter Eckersley, How Unique Is Your Web Browser? (2010)<br><a href="https://panopticlick.eff.org/browser-uniqueness.pdf">https://panopticlick.eff.org/browser-uniqueness.pdf</a>                                                                                                                                                     | The Panopticlick study: 470,161 browsers, 83.6% with a unique fingerprint, how fingerprints change, and how changed fingerprints can still be matched. |
| [12] | Electronic Frontier Foundation, press release on the Panopticlick findings (May 2010)<br><a href="https://www.eff.org/press/archives/2010/05/13">https://www.eff.org/press/archives/2010/05/13</a>                                                                                                                                   | EFF's summary of the study, including that fingerprints must be considered alongside cookies and IP addresses.                                         |
| [13] | Laperdrix, Bielova, Baudry and Avoine, Browser Fingerprinting: A Survey (2020)<br><a href="https://arxiv.org/abs/1905.01051">https://arxiv.org/abs/1905.01051</a>                                                                                                                                                                    | A review of fingerprinting techniques, studies and defenses.                                                                                           |
| [14] | Electronic Frontier Foundation, Cover Your Tracks<br><a href="https://coveryourtracks.eff.org/">https://coveryourtracks.eff.org/</a>                                                                                                                                                                                                 | A tool that tests how well a browser resists tracking and fingerprinting.                                                                              |
| [15] | AmlUnique<br><a href="https://amiunique.org/">https://amiunique.org/</a>                                                                                                                                                                                                                                                             | A research project and tool for checking how unique a browser fingerprint is.                                                                          |
| [16] | European Data Protection Board, Report of the work undertaken by the Cookie Banner Taskforce (January 2023)<br><a href="https://www.edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf">https://www.edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf</a> | Pre-ticked boxes are not valid consent, and most authorities expect a reject option as easy to use as accept.                                          |
| [17] | Bird & Bird, Planet49: CJEU rules on cookie consent (2019)<br><a href="https://www.twobirds.com/en/news/articles/2019/global/planet49-cjeu-rules-on-cookie-consent">https://www.twobirds.com/en/news/articles/2019/global/planet49-cjeu-rules-on-cookie-consent</a>                                                                  | The EU court ruling that pre-ticked checkboxes are not valid consent for cookies.                                                                      |
| [18] | Global Privacy Control<br><a href="https://globalprivacycontrol.org/">https://globalprivacycontrol.org/</a>                                                                                                                                                                                                                          | The browser signal for opting out of the sale or sharing of personal data.                                                                             |
| [19] | California Attorney General, announcement of the Sephora settlement as part of ongoing CCPA                                                                                                                                                                                                                                          | California's position that businesses must honor user-enabled global privacy controls.                                                                 |