

INSTRUCTOR GUIDE AND NOTES

Cookies and fingerprints

A Take Back Your Bytes lesson: how websites recognize you with cookies, user agents and browser fingerprints, and what you can do about it. A 50-minute lesson with a lab, a hands-on look at your own browser, and discussion.

Series	Take Back Your Bytes, PrivacySafe Foundation's cybersecurity education campaign ^[20]
Audience	Teens and adults. No technical background needed. Adapt the language for younger learners.
Length	50 minutes, with a 30-minute cut
Format	4 slides, live cookie lab, 4 slides, hands-on browser check, discussion
You will need	Slides (light for print, dark for projecting), the cookie lab served over HTTP or HTTPS, flash cards, and learners' own browsers
Facts checked	October 27, 2026. Browser defaults and menus change. Re-check before you teach.

PrivacySafe Foundation, Inc. | Take Back Your Bytes | 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. Names of browsers, tools and projects belong to their owners and are used as examples.

The lesson in five sentences

1. A cookie is a small piece of text a site asks your browser to keep and send back, and it is only as harmful as the ID it carries^{[1][2][3]}.
2. A third party that appears on many sites can set the same cookie everywhere, link your visits and build a profile^[4].
3. Browsers differ on third-party cookies: some block or separate them by default, and others leave the choice to you^{[5][6][7]}.
4. Your browser also tells every site its user agent and many small details, and together they can form a fingerprint that needs no cookie^{[8][9][11][13]}.
5. No single control solves this: combine cookie settings, careful banner choices, the Global Privacy Control and a common, up-to-date browser, and review them regularly^{[14][18]}.

LEARNING OUTCOMES

By the end, students can:

1. Describe how a cookie is set, stored and sent back, and what its main settings mean^{[1][2]}.
2. Explain how a third-party cookie lets a company follow you across sites^[4].
3. Read a user agent string and say what it reveals^{[8][9]}.
4. Explain browser fingerprinting and why deleting cookies does not stop it^{[11][13]}.
5. Choose realistic controls and say what trade-off each brings.

Session plan

SEGMENT	MINUTES	NOTES
Before the demo, slides 1 to 4	12	Includes the prediction: can a site recognize you after you delete cookies?
Cookie lab	12	Sections 1 to 4. Section 5 feeds the hands-on check.
After the demo, slides 1 to 4	10	Controls, user agent, fingerprinting, plan.
Hands-on browser check	10	Learners choose a check. Taking part is optional.
Discussion	6	Two questions.

30-MINUTE CUT

Skip the hands-on check and show one on the instructor browser. In the lab, do sections 1, 2 and 4. Cover after-demo slides 1 and 3. Use one discussion question.

Before class

- Optional: the lesson page has a walkthrough video of under five minutes, in a light version for the page and a dark version for projecting, each with a subtitles file. Play it as a recap, or share it with learners who missed the session. Check that it plays on the room computer first.
- **Serve the lab over HTTP or HTTPS.** Browsers do not keep cookies for a page opened straight from a file, so the lab would show only its message about that. HTTPS also lets the lab use the Secure attribute and a SHA-256 hash for the fingerprint ID^[2].
- Open the lab and try each section. Press Set the cookie, tick the visit counter, reload, then delete cookies and recompute the fingerprint. Set browser zoom to about 125% for the back row.
- **Explain what the lab does.** It sets cookies on the learner's own browser only when they press a button or tick a box. They hold a random value and a counter. As with any cookie, the browser sends them back to the lesson site with later requests, which the wire box in the lab shows, and nothing else reads them. The lab sets no cookie on load. Tell learners they can delete them with the button.
- **Check device policy.** Do not change settings on school or work devices without permission. Offer a demonstration on the instructor browser for anyone who cannot or does not want to take part.
- Read the current pages on cookie settings for the browsers in the room^{[5][6][7]}. Defaults and menus change.
- Print the flash cards, double-sided, flipped on the long edge.

TEACH IT FAIRLY

- **Cookies are not the enemy.** Many keep you signed in and remember choices. The concern is third parties and unique IDs^{[1][4]}.
- **Tools are examples.** Cover Your Tracks and AmlUnique are examples of fingerprint tests^{[14][15]}. Present results as estimates and invite learners to compare.
- **Avoid absolutes.** A fingerprint is not a guaranteed ID. Fingerprints change, and defenses vary^{[11][13]}.
- **Fingerprinting is a real concern for sites too.** Some uses are for fraud detection and security. The privacy concern is tracking without a clear choice.

WHAT THE LAB IS, AND IS NOT

The cookie in section 1 is real and is set only in the learner's browser. Section 3 reads the learner's real user agent. Section 4 reads real details from the learner's browser, including screen size, time zone, languages, fonts and graphics. The ID is made in the browser and not sent anywhere. The three sites and the ad company in section 2, and the shares in the crowd example in section 4, are made up. Real fingerprinting uses many more details, and some privacy-focused browsers hide or randomize them, so results differ by browser. Treat the lab as an illustration of the mechanism and not a measurement of how unique the learner's browser is.

Slide notes: before the demo

Slide 1: Title

about 2 min

SAY

How does a website know it is you, even after you leave and come back? Our 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. The four-segment bar is the plan: cookie, user agent, fingerprint, controls.

DO

Introduce Take Back Your Bytes as the Foundation's cybersecurity education campaign^[20].

CHECK FOR UNDERSTANDING

Ask: "What do you think a cookie is? Where does it live?"

Slide 2: What a cookie is

about 4 min

SAY

1. The browser asks for a page.
2. The server replies with a `Set-Cookie` header.
3. The browser stores the cookie.
4. Every later request to that site carries it in a `Cookie` header^{[1][3]}.

A cookie has a name and a value, and settings: Domain and Path (where it is sent), Max-Age or Expires (how long), Secure (HTTPS only), HttpOnly (hidden from page scripts) and SameSite (whether it is sent on cross-site requests)^[2]. Without a lifetime it is a session cookie. Third-party cookies are set by an outside company on a page you chose to visit^[4].

DO

Draw the four steps. Point out that a cookie is only text and cannot run code.

CHECK FOR UNDERSTANDING

Ask: "If a cookie is just text, why does it matter?" Because the value can be a unique ID.

WATCH FOR

Do not say cookies are programs or viruses. They are not. Also avoid calling all cookies tracking: sign-in and shopping carts depend on them.

Slide 3: How cookies become tracking

about 4 min

SAY

Three sites each load code from the same ad company. The company sets one cookie with an ID, the browser sends it from every site, and the company links the visits into one profile^[4]. Companies can also swap IDs to match profiles, which is called cookie syncing. Browsers differ: Safari blocks third-

party cookies by default^[5], Firefox blocks cross-site tracking cookies and isolates cookies per site^[6], and Chrome gives you the option to block them^[7].

DO

Walk the diagram. Ask learners to say what the ad company learned that none of the three sites knew alone.

CHECK FOR UNDERSTANDING

Ask: "Deleting cookies resets the ID. Does that stop tracking?" Hold the answer for the demo.

WATCH FOR

Browser behavior changes, and secondary sources disagree. State what each vendor's own page says and tell learners to check their browser.

Slide 4: What to watch for, and the prediction

about 2 min

SAY

Your cookie: a real one, what it stores, how long it lasts, what the browser sends back, and how a tracker can follow one. 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, and how narrowing a crowd works.

DO

Read the prediction: "If you delete all your cookies, can a website still recognize your browser?" Collect yes or no and a reason.

WATCH FOR

Many learners say no. Some say yes through an account or IP address. Both are partly right, and the lab shows the fingerprint route.

Cookie lab script (about 12 minutes)

Section 1: Show a cookie

4 min

SAY

Leave the options as they are and press **Set the cookie**. The card shows the real cookie in your browser: name, random value, site, path, lifetime, Secure and SameSite. The wire box shows the `Set-Cookie` line the server would send once, and the `Cookie` line the browser sends on later requests^{[1][2]}. Press Reload, and the cookie is still there. Try 5 minutes or 1 day, and SameSite None, which needs Secure and therefore HTTPS.

DO

Tick the visit counter, reload, and watch it say "welcome back": that is how a site recognizes a returning browser. Press Delete the cookie: the lab sets it to expire at once, with `Max-Age=0`^[2].

CHECK FOR UNDERSTANDING

Ask: "Why can the page not set HttpOnly?" Only a server can, through the header, and it hides the cookie from page scripts^[1].

WATCH FOR

On a page opened from a file, or with cookies blocked, the lab says it cannot set cookies. That is expected.

Section 2: Follow a tracker across sites

3 min

SAY

Press the three site buttons with **Third-party cookies allowed**. The ad company sees one cookie ID on all three and builds one profile: cooking, local news and hiking boots. Switch to **blocked**, start over and visit again: it believes it saw three visitors. Choose **partitioned**: each site gets a different cookie, with the same result^{[4][2]}.

DO

Tick "The ad company also collects a browser fingerprint": the three visits join into one visitor again. Press Delete all cookies in the allowed mode to show an ID reset.

CHECK FOR UNDERSTANDING

Ask: "What did blocking cookies protect, and what did it not?" It broke the cookie link but not a fingerprint link.

WATCH FOR

This simulation is made up and simplified. Real tracking also uses IP addresses, accounts and other signals.

Section 3: Your user agent

2 min

SAY

The lab prints your browser's real User-Agent string and splits it into parts. `Mozilla/5.0` is a historical token that almost every browser sends^[8]. The system details name the operating system, and the engine, browser and version follow. The page also shows Client Hints if your browser offers them^[10]. Open the examples: a reduced Chrome string shows minor versions as zeros and hides the device model^[9].

CHECK FOR UNDERSTANDING

Ask: "What can a site guess from this without asking you?" Browser, version, operating system and whether it is a phone.

WATCH FOR

The parsing is a simple guess from patterns. Do not use it as a reliable detector. MDN advises feature detection over user agent sniffing^[9].

Section 4: Your fingerprint

3 min

SAY

The lab reads real details from your browser and combines them into an ID. Read a few rows aloud and note which ones the lab marks as identifying more: fonts, canvas drawing and graphics, then user agent and screen, then languages and time zone. Press **Delete my cookies, then recompute**: the ID is the same, so a site could still recognize this browser. That answers the prediction.

DO

Press "Change one detail and recompute": a small change gives a completely different ID, and real fingerprints drift, so trackers match similar ones^[11]. Then tick the crowd boxes one by one: each detail narrows a crowd of 1,000,000 until you are likely unique. The shares are made up.

CHECK FOR UNDERSTANDING

Ask: "What would you change to make your browser look like many others?" Keep common settings, update the browser, avoid unusual add-ons.

WATCH FOR

Some browsers return generic or randomized values for canvas, fonts or graphics, so learners may see different results. Use that as a talking point about built-in protection^[13].

Section 5: Make your plan

1 min

SAY

Choose a browser. The page builds a checklist: today, this week, every few months. Learners can tick items and copy the plan.

DO

Hand over to the hands-on check.

Close the prediction

1 min

SAY

Yes. Deleting cookies resets cookie IDs, but a site can still recognize your browser by its fingerprint, and also by your IP address or an account you sign in to^{[11][12]}.

DO

Return to slide 4 and compare answers.

Slide notes: after the demo

Slide 1: Cookie controls

about 3 min

SAY

CONTROL	TEACHING POINT
Block third-party cookies	Stops outside companies from setting cookies they read across sites. Some embedded logins or comments may break ^[4] .
Separate cookies per site	The same company gets a different cookie on each site, so it cannot match them. Firefox does this by default ^[6] . Cookies can also opt in with the Partitioned attribute ^[2] .
Clear cookies	Resets IDs and signs you out. A fingerprint can still link you.
Choose Reject on banners	Optional cookies stay off. In the EU, pre-ticked boxes are not valid consent ^{[16][17]} , and most data protection authorities expect a reject option on the first layer ^[16] .
Global Privacy Control	A browser signal asking sites not to sell or share your data ^[18] . California's Attorney General says businesses must honor it ^[19] .
Separate profiles	Keeps school, work and shopping apart.

CHECK FOR UNDERSTANDING

Ask: "Which of these would you actually use, and why?" Realistic choices beat a long list.

WATCH FOR

Browsers differ, and defaults change. Do not tell the room what their browser does. Send them to the vendor pages.

Slide 2: The user agent string

about 3 min

SAY

The string is sent with every request. It names the browser, version, engine and operating system.

`Mozilla/5.0` is there for historical reasons^[8]. Some browsers now reduce it, hiding exact OS version, device model and minor version, and sites that need more can ask for User-Agent Client Hints^{[9][10]}. Sites use it for compatibility and statistics. It also adds to a fingerprint, and it can be changed. Changing it can make you stand out.

CHECK FOR UNDERSTANDING

Ask: "Why do so many browsers still say Mozilla?" Old websites checked for it, so browsers kept sending it.

WATCH FOR

Do not suggest that changing the string makes anyone anonymous.

Slide 3: Browser fingerprinting

about 4 min

SAY

A fingerprint combines many small details: user agent, language, time zone, screen size, fonts, canvas drawing, graphics hardware and add-ons. It needs no cookie. In EFF's 2010 Panopticlick study of 470,161 browsers, 83.6% had a fingerprint that was unique in the sample, and 94.2% among those with Flash or Java enabled^{[11][12]}. Fingerprints change over time, but the study found that changed ones could often still be matched^[11]. The survey literature describes many more techniques and defenses^[13].

DO

Defenses: common settings, a current browser, a browser with built-in anti-fingerprinting protection, and few unusual add-ons. Test your browser with Cover Your Tracks or AmlUnique, and treat results as estimates^{[14][15]}.

CHECK FOR UNDERSTANDING

Ask: "Why can a random fake value make you more unique?" Because few other browsers would show it.

WATCH FOR

The 2010 numbers are historical and came from a sample of people interested in privacy. Say so, and do not present them as today's rates.

Slide 4: Your cookie plan

about 4 min

SAY

1. Look at the cookies on a site you use.
2. Check your browser's third-party cookie setting.
3. Clear cookies you do not need.
4. Choose Reject on cookie banners when you can.
5. Turn on the Global Privacy Control if offered.
6. Test your browser's fingerprint.
7. Keep your browser updated, with few unusual add-ons.
8. Use separate profiles for school, work and home.

DO

Introduce the hands-on check below.

Hands-on browser check (about 10 minutes)

Learners choose one check on their own browser. Taking part is optional, and nobody has to show their own accounts or settings.

1. **Look at a cookie.** Open a site you use. In developer tools, open the Application or Storage tab and choose Cookies. Pick one cookie and note its name, domain, lifetime, Secure and SameSite settings. Compare with the lab^{[1][2]}.
2. **Check a setting.** Find your browser's third-party cookie setting and note what it is set to^{[5][6][7]}.
3. **Test your fingerprint.** Run Cover Your Tracks or AmlUnique and note what it says about your browser^{[14][15]}. Then close the tab. Treat the result as an estimate.
4. **Read a banner.** Visit a site with a cookie banner. Find the Reject option and note how easy it was to find^[16].
5. **Count cookies.** Visit a news site and count the cookies in developer tools, then count how many belong to other domains.

TROUBLESHOOTING

- The lab will not set a cookie. Check that it is served over HTTP or HTTPS and that cookies are allowed for the site.
- The fingerprint ID differs between browsers on the same computer. That is expected: each browser reports its own details.
- A fingerprint test says "unique" for a common setup. Small samples and unusual settings can skew results, so compare tools.
- Developer tools look different in each browser. Use the browser's help to find the cookie storage view.

Discussion (about 6 minutes)

QUESTION 1: DO BANNERS GIVE A CHOICE?

"Cookie banners are meant to give you a choice. Do they? What would a better design look like?"

- In the EU, pre-ticked boxes are not valid consent, and most authorities expect reject to be as easy as accept^{[16][17]}.
- Ask for examples of banners that make rejecting hard.
- Ideas for better design: one-click reject, plain language, and a browser-level signal that sites must honor^[18].

QUESTION 2: WHO ELSE SHOULD ACT?

"A fingerprint works without cookies and is hard to stop. Who else should act: browser makers, websites or lawmakers?"

- Browser makers can reduce what is exposed, as user agent reduction does^[9].
- Websites and ad companies can choose not to fingerprint, and laws can limit it.
- Individuals can choose common settings and keep browsers updated. There is no single answer.

Answer key and assessment

QUESTION	ANSWER
What is a cookie?	A small piece of text a site asks the browser to keep and send back ^[1] .
What makes a cookie a tracker?	A unique ID, usually set by a third party that appears on many sites ^[4] .
How do you delete a cookie from JavaScript?	Set it again with Max-Age=0 ^[2] .
Can a site recognize you after you delete cookies?	Yes, through a fingerprint, an IP address or an account ^[11] .
What is in a user agent string?	Browser, version, engine and operating system, plus the historical Mozilla/5.0 ^[8] .
What helps against fingerprinting?	Common settings, an updated browser, built-in protection and few unusual add-ons ^[13] .

EXIT TICKET (3 MINUTES)

1. Name one good use of a cookie and one tracking use.
2. Why does deleting cookies not stop fingerprinting?
3. Write one action you will take this week.

HOMEWORK

- Complete your plan from section 5 and report which steps you did.
- Run a fingerprint test in two browsers. Describe what is different and why.
- Stretch: find the privacy policy of a site you use and note what it says about cookies.

Common questions and misconceptions

QUESTION OR BELIEF	RESPONSE
"Cookies are programs."	They are text. They cannot run code. The risk is the ID they carry ^[1] .
"Deleting cookies makes me anonymous."	It resets cookie IDs. Fingerprints, IP addresses and accounts can still recognize you ^{[11][12]} .
"Private browsing stops fingerprinting."	It mainly stops your device saving history. Sites can still see your browser's details.
"Changing my user agent hides me."	It can make you more unusual. Many sites also use other details ^{[9][13]} .

"Rejecting cookies breaks every site."

Essential cookies still work. Many sites work fine with optional ones off.

"A fingerprint test result is exact."

It is an estimate from a limited sample and the details a tool collects^[13].

References and further reading

Citations in this guide use bracketed numbers. Links were checked on October 27, 2026. Browser behavior and menus change, so confirm details before you teach. The fingerprinting figures come from a 2010 study and are historical.

#	SOURCE	WHAT IT SUPPORTS
[1]	MDN Web Docs, Using HTTP cookies https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/Cookies	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 https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie	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 https://www.rfc-editor.org/rfc/rfc6265	The standard that defines cookies.
[4]	MDN Web Docs, Third-party cookies https://developer.mozilla.org/en-US/docs/Web/Privacy/Third-party_cookies	How third-party cookies enable cross-site tracking, and how browsers respond.
[5]	WebKit, Full Third-Party Cookie Blocking and More https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/	Safari's default blocking of third-party cookies.
[6]	Mozilla Support, Third-party cookies and Firefox tracking protection https://support.mozilla.org/en-US/kb/third-party-cookies-firefox-tracking-protection	Firefox's default protection against cross-site tracking cookies.
[7]	Google Chrome Help, Manage cookies in Chrome https://support.google.com/chrome/answer/95647	Chrome's cookie settings, including the option to allow or block third-party cookies.
[8]	MDN Web Docs, User-Agent header https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/User-Agent	The format of the User-Agent header and the historical Mozilla/5.0 token.
[9]	MDN Web Docs, User-Agent reduction https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/User-agent_reduction	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 https://developer.mozilla.org/en-US/docs/Web/API/User-Agent_Client_Hints_API	The navigator.userAgentData interface and low-entropy versus high-entropy values.

[11]	Peter Eckersley, How Unique Is Your Web Browser? (2010) https://panopticklick.eff.org/browser-unique-ness.pdf	The Panopticklick 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 Panopticklick findings (May 2010) https://www.eff.org/press/archives/2010/05/13	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) https://arxiv.org/abs/1905.01051	A review of fingerprinting techniques, studies and defenses.
[14]	Electronic Frontier Foundation, Cover Your Tracks https://coveryourtracks.eff.org/	A tool that tests how well a browser resists tracking and fingerprinting.
[15]	AmIUnique https://amiunique.org/	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) https://www.edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf	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) https://www.twobirds.com/en/news/articles/2019/global/planet49-cjeu-rules-on-cookie-consent	The EU court ruling that pre-ticked checkboxes are not valid consent for cookies.
[18]	Global Privacy Control https://globalprivacycontrol.org/	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 enforcement https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement	California's position that businesses must honor user-enabled global privacy controls.
[20]	PrivacySafe Foundation https://privacysafe.foundation/	The Take Back Your Bytes education campaign and the Foundation's other work.
[21]	Creative Commons, CC0 1.0 Universal https://creativecommons.org/publicdomain/zero/1.0/	The public-domain dedication that covers these lesson materials.

ABOUT THESE MATERIALS

The slides, lab, flash cards and this guide were written for the PrivacySafe Foundation's Take Back Your Bytes campaign. They are dedicated to the public domain under CC0 1.0^[21]. The Foundation names and logos are trademarks and are not included in that dedication. This lesson is independent of the projects and organizations named in the references.