

# Web UI Attacks & Privacy

## CMSC 23200, Spring 2025, Lecture 13

---

Grant Ho

University of Chicago, 05/06/2025

(Slides adapted from Blasé Ur, Peyrin Kao, Vern Paxson, and Zakir Durumeric)

# Logistics

- Assignment 5 released either Fri / Sat (May 9 / 10)
  - Due Thursday, May 15 by 11:59pm
  - Schedule change due to VM outage
  - No TA office hours this week
- Discussion Section #5 tomorrow (May 7)

# Outline

- UI Attacks
  - Clickjacking Attacks
  - Phishing Attacks
- Web Privacy: Online Tracking

# Misleading Users

- **UI Attacks**: trick the victim into thinking they are taking an **intended** action, when they are actually taking a **malicious** action
  - **Clickjacking**: Trick the victim into clicking on some website element
  - **Phishing**: Impersonate another entity & trick victim into performing specific malicious actions (e.g., giving sensitive information)
- Key Issue: Browser assumes clicks & keystrokes = *clear indication of user's intended actions*
  - Constitutes part of the user's *trusted path*

# Clickjacking

- Trick the victim into clicking on something from the attacker by hiding one frame (origin A) on-top or underneath another (origin B)
- Why steal clicks?
  - Download a malicious program
  - Like a YouTube video
  - Delete an online account
- Why steal keystrokes?
  - Steal passwords
  - Steal credit card numbers
  - Steal personal info

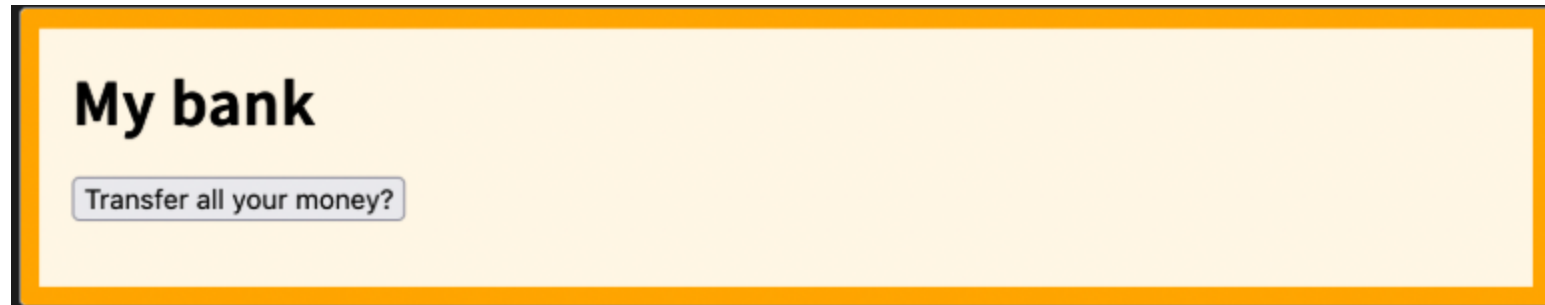


# Clickjacking Example

Suppose you use *cheapbank.com*... and they have a transfer page!

URL: `https://cheapbank.com/transfer.html?receiver=...`

Resulting  
webpage in  
browser  
(includes  
CSRF token)



Example from: <https://developer.mozilla.org/en-US/docs/Web/Security/Attacks/Clickjacking>

# Clickjacking Example

Attacker on *shady-pet-supplies.com* creates a webpage with the following HTML & CSS:

## HTML:

```
<button id="fake-button">Click here for a free kitten!</button>  
<iframe width="800" height="200" src="https://cheapbank.com/transfer.html?receiver=attacker"></iframe>
```

## CSS:

```
#fake-button {  
  position: absolute; top: 185px; left: 90px;    <----- Overlay attack button exactly over framed button  
}
```

# Clickjacking Example

`shady-pet-supplies.com`

**Get a free kitten!**



SOP prevents *shady-pet-supplies.com* from interacting with embedded iframe – but user allowed to click & interact however they want!



# Clickjacking Example

Attacker on *shady-pet-supplies.com* creates a webpage with the following HTML & CSS:

## HTML:

```
<button id="fake-button">Click here for a free kitten!</button>  
<iframe width="800" height="200" src="https://cheapbank.com/transfer.html?receiver=attacker"></iframe>
```

## CSS:

```
iframe { opacity: 0; }      <----- Invisible iframe contents  
  
#fake-button {  
  position: absolute; top: 185px; left: 90px;   <----- Overlay attack button exactly over framed button  
}
```

# Clickjacking Example

shady-pet-supplies.com

**Get a free kitten!**

iframe = top most element,  
but hidden / invisible with:  
`iframe { opacity: 0; }`

**My bank**

`https://cheapbank.com/transfer.html?receiver=...`

Transfer all your money?

# Clickjacking Example

shady-pet-supplies.com

**Get a free kitten!**

My bank

`https://cheapbank.com/transfer.html?receiver=...`

Click here for a free kitten!

# Clickjacking: Multiple Attack Variants

- By placing an **invisible** iframe of `target.com` **over** some enticing content, a malicious web server can fool a user into taking unintended action on `target.com` ...
- By placing a **visible** iframe of `target.com` **under** the *attacker's own invisible iframe*, a malicious web server can “steal” user input (**keystrokes**)
  - Input text will be entered on the attacker site's iframe/origin

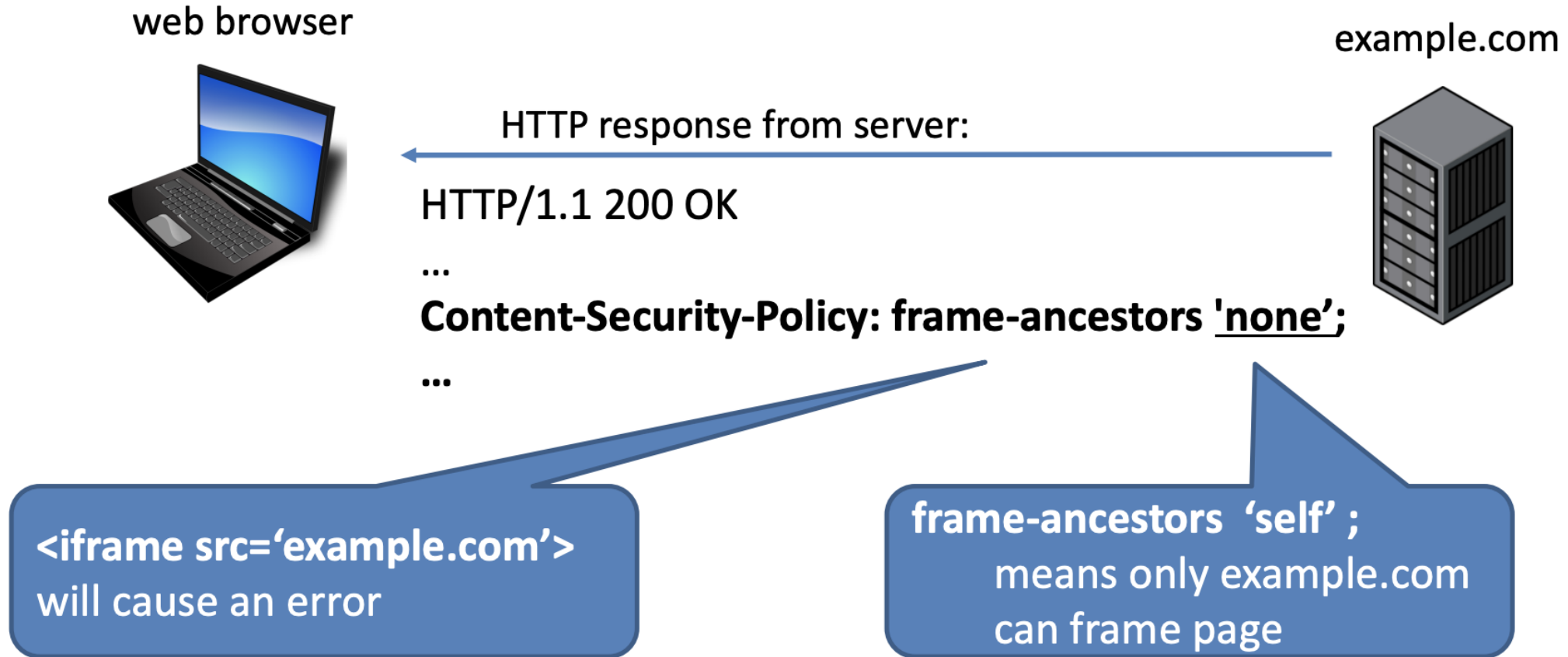
# Defenses:

## Prevent Other Sites from Framing You!



Attacker implements clickjacking by placing target's page (e.g., Twitter) in a "frame" inside their own page. Otherwise they wouldn't overlap.

# Defenses: CSP or HTTP X-Frame-Options



# Outline

- UI Attacks
  - Clickjacking Attacks
  - Phishing Attacks
- Web Privacy: Online Tracking

# Phishing

- Masquerade as a reputable entity & trick the user into performing malicious actions, such as divulging login credentials
- Often easier than attacking the security of a system directly
  - Just get the user to tell you their password or download & run your malicious software



Dear vern we are making a few changes

[View Online](#)



# Your Account Will Be Closed !

Hello, Dear vern

Your Account Will Be Closed , Until We Here From You . To Update Your Information . Simply click on the web address below

**What do I need to do?**

[Confirm My Account Now](#)

Date: Thu, 9 Feb 2017 07:19:40 -0600

From: PayPal <alert@gnc.cc>

Subject: [Important] : This is an automatic message to : (vern)

To: vern@aciri.org

ern". Emails from PayPal will always address you by your

This email was sent to vern.

Copyright Â(c) 1999-2017. All rights reserved. PayPal Pte. Ltd. Address is 5 Temasek Boulevard #09-01 Suntec Tower 5 Singapore 038985

Dear vern we are making a few changes

[View Online](#)



# Your Account Will Be Closed !

Hello, Dear vern

Your Account Will Be Closed , Until We Here From You . To Update Your Information . Simply click on the web address below

**What do I need to do?**

[Confirm My Account Now](#)



[Help](#) [Contact](#) [Security](#)

## How do I know this is not a Spoof email?

Spoof or 'phishing' emails tend to have generic greetings such as "Dearvern". Emails from PayPal will always address you by your first and last name.

[Find out more here.](#)

This email was sent to vern.

Copyright Â(c) 1999-2017. All rights reserved. PayPal Pte. Ltd. Address is 5 Temasek Boulevard #09-01 Suntec Tower 5 Singapore 038985

Open "universalkids.com.br/re.php" in a new window



**Log In**

[Forgot your email or password?](#)

**Sign Up**



gaga@lady.com

.....

Log In

[Forgot your email or password?](#)

Sign Up



Email

Password

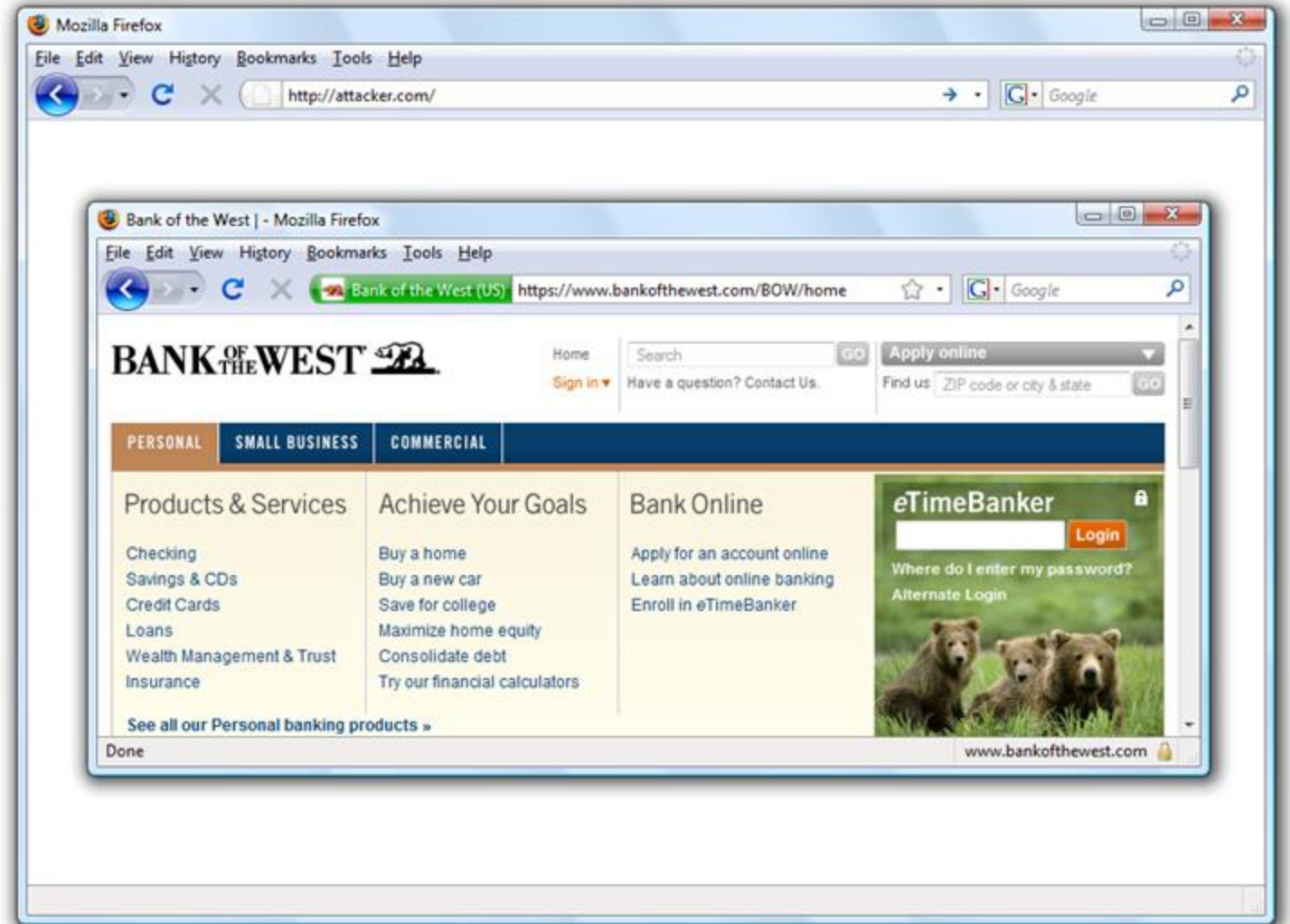
Log In

[Having trouble logging in?](#)

Sign Up

# Lots of Phishing Strategies

**Browser-in-browser attack:**  
The attacker simulates the entire web browser with JavaScript



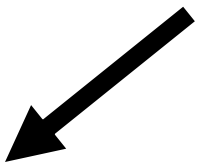
# Internationalized Domain Names (IDN)

- Domain names consist of ASCII characters
- Hostnames containing Unicode characters are transcoded to subset of ASCII consisting of letters, digits, and hyphens called punycode
- Allows registering domains with foreign characters!
  - münchen.example.com → xn--mnchen-3ya.example.com

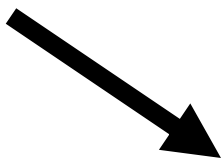
# Phishing: IDN homograph attack

- Many Unicode characters are difficult to distinguish from common ASCII characters

apple.com vs. apple.com



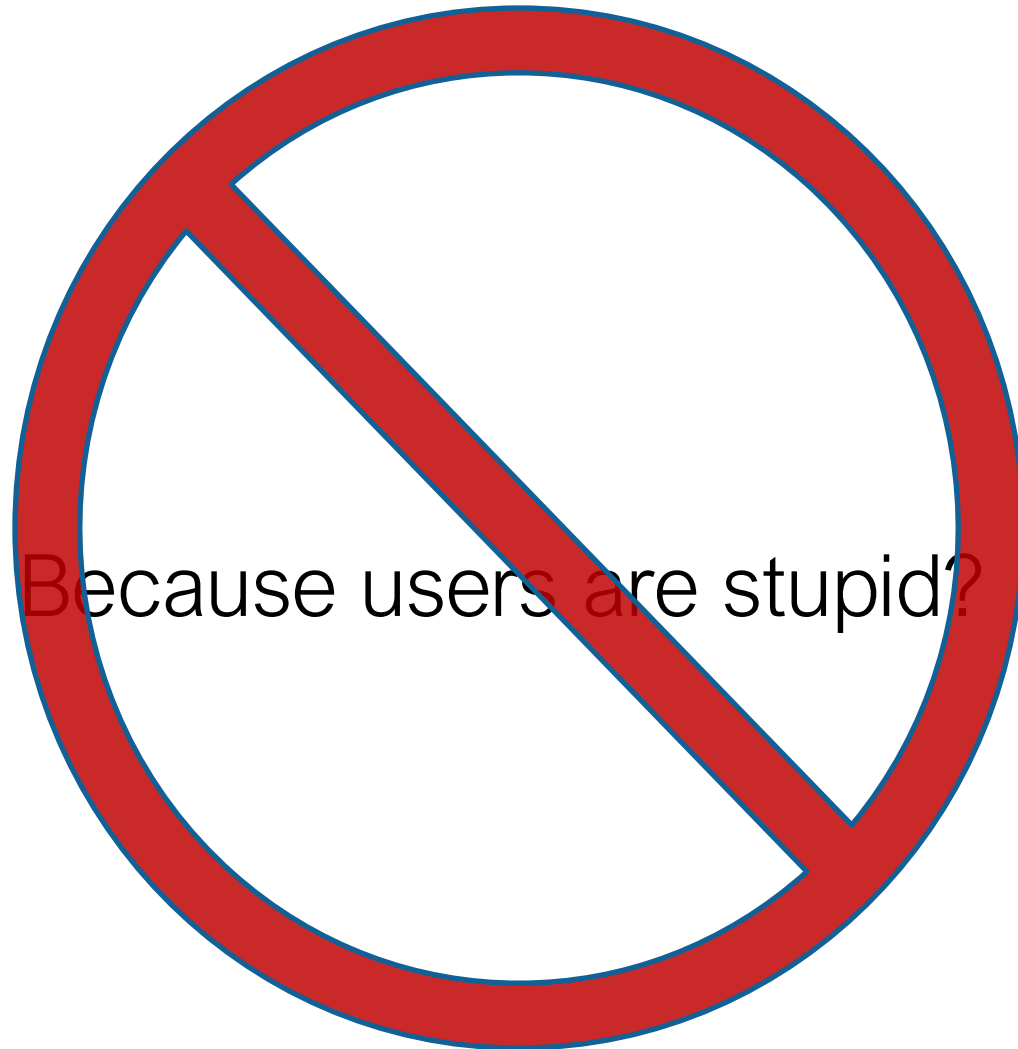
xn--ppl-43d.com



apple.com



# Why does phishing work?

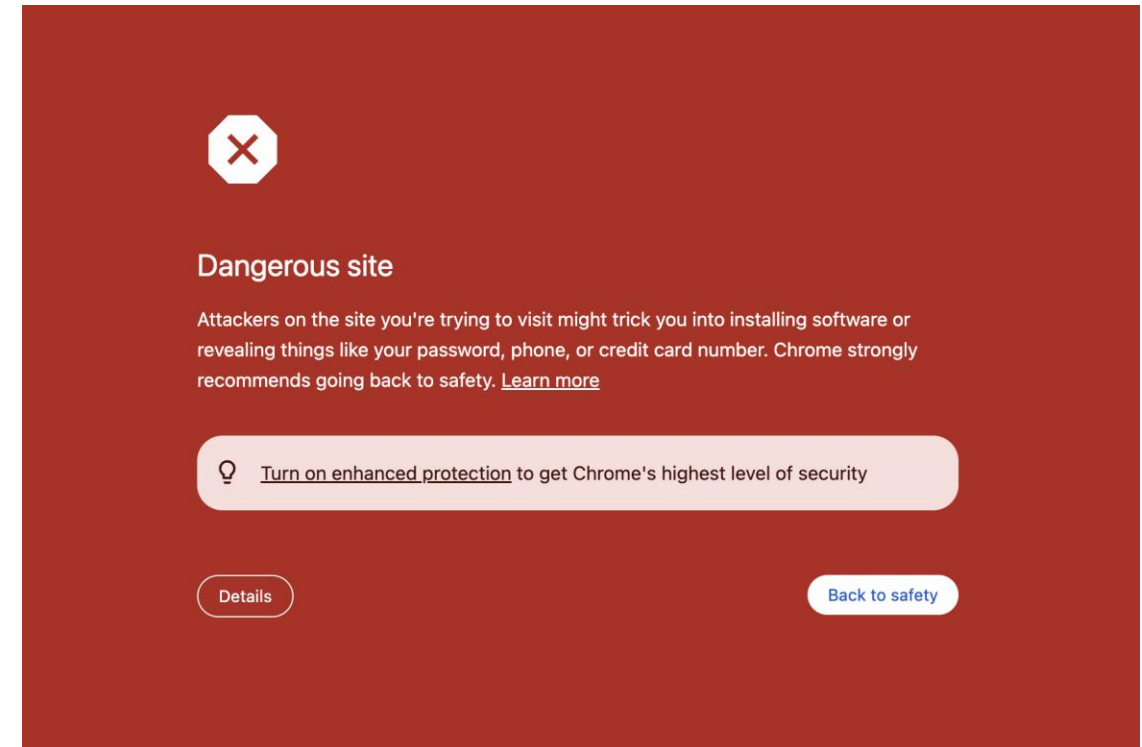
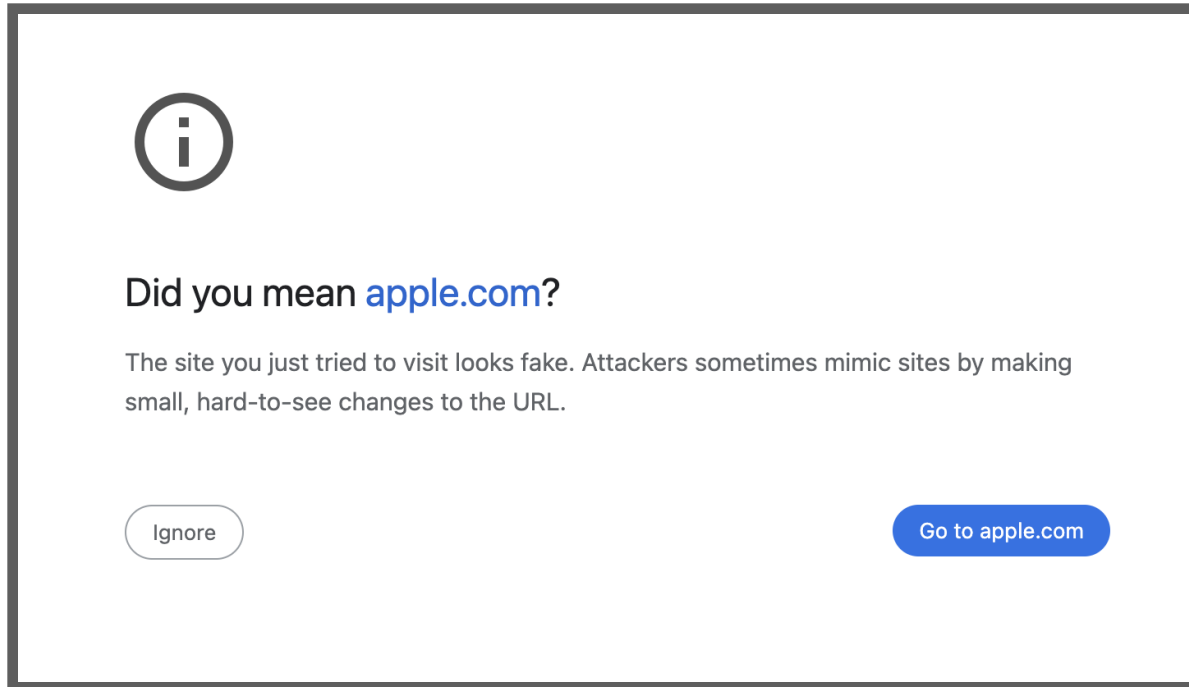


# Why does phishing work?

- User **mental model** vs. reality
  - Browser security model too hard to understand!
  - Phishing is hard to spot even if you're an expert!
- The easy path is insecure; the secure path takes **extra effort**
- Risks are **rare**
- Users tend not to suspect malice; they find benign interpretations and have been *acclimated to failure*

# Phishing Defenses

- Detection & Blocklists (e.g., Google Safe Browsing)



# Phishing Defenses

- Detection & Blocklists (e.g., Google Safe Browsing)
- Next week:
  - Password Managers (for credential phishing)
  - Multi-factor authentication (your friend Duo!)

# Outline

- UI Attacks
  - Clickjacking Attacks
  - Phishing Attacks
- Web Privacy: Online Tracking

# Online Tracking

- Advertisers want to show you advertisements targeted to your interests and demographics

The screenshot displays the 'Ads Preferences' page on Google. At the top, there's a navigation menu with 'Ads on Search and Gmail' and 'Ads on the web' (which is selected). Below this, the main heading is 'How your ads are personalized'. A paragraph explains that ads are based on personal info from the Google Account, advertiser data, and Google's interest estimation. A 'Learn more' link is provided. Below this is a grid of 20 interest categories, each with an icon and a label: Accounting & Finance Jobs, Action & Platform Games, Android OS, Banking, Beaches & Islands, Bollywood & South Asian Film, Business & Productivity Software, Action & Adventure Films, Adventure Games, Autos & Vehicles, Bars, Clubs & Nightlife, Blues, Books & Literature, and Business News. To the right of the grid, there's a section for 'Your categories' which lists various interests like Arts & Entertainment, Computers & Electronics, Internet & Telecom, etc. Below that is a section for 'Your demographics' showing 'Age: 35-44' and 'Gender: Male'. A 'Google' logo is visible in the bottom right corner.

**Ads Preferences**

- Ads on Search and Gmail
- Ads on the web**
- Opt out

**How your ads are personalized**

Ads are based on personal info you've added to your Google Account, data from advertisers that partner with Google, and Google's estimation of your interests. Choose any factor to learn more or update your preferences. [Learn more](#)

Accounting & Finance Jobs

Action & Platform Games

Android OS

Banking

Beaches & Islands

Bollywood & South Asian Film

Business & Productivity Software

Action & Adventure Films

Adventure Games

Autos & Vehicles

Bars, Clubs & Nightlife

Blues

Books & Literature

Business News

**Ads on the web**

**Make the ads you see on the web more interesting**

Many websites, such as news sites and blogs, partner with us to show ads to their visitors. To see ads that are more related to you and your interests, edit the categories below, which are based on sites you have recently visited. [Learn More](#)

Your interests are associated with an advertising cookie that's stored in your browser. If you don't want us to store your interests, you can opt out below. Your ads preferences only apply in this browser on this computer. They are reset if you delete your browser's cookies.

[Watch a video: Ads Preferences on GDN explained](#)

**Your categories**

Below you can review the interests and inferred demographics that Google has associated with your cookie. You can [remove](#) or [edit](#) these at any time.

Arts & Entertainment

Computers & Electronics

Computers & Electronics - Consumer Electronics - Gadgets & Portable Electronics - PDAs & Handhelds

Internet & Telecom

Internet & Telecom - Mobile & Wireless - Mobile Phones - Smart Phones

Law & Government

Science

**Your demographics**

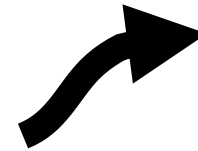
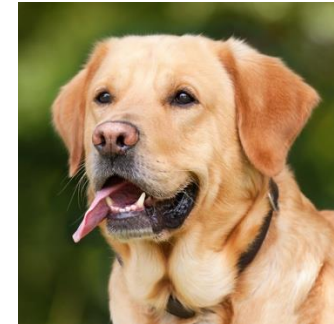
We infer your age and gender based on the websites you've visited. You can [remove](#) or [edit](#) these at any time.

Age: 35-44

Gender: Male

Google

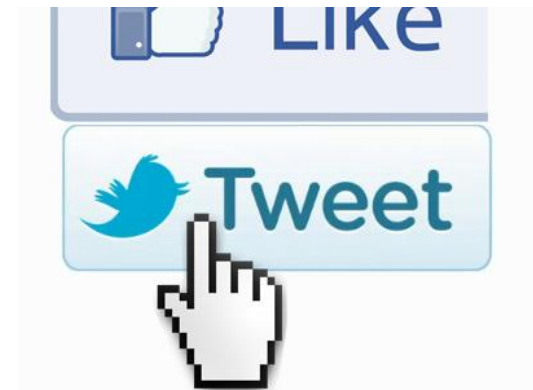
# Data-Driven Inferences



You might like dogs!

# Online Tracking

- First party: the site you are visiting (address in the URL bar)
  - First-party tracking (on search engines, shopping sites)
  - Login/Session cookies
- Third party: other sites (origins) embedded/contacted by the first party site you're visiting
  - Third-party tracking (ads on lots of sites)





# Online Tracking

The image shows a screenshot of the New York Times website with several annotations illustrating online tracking concepts:

- 1st Party:** A blue box on the left with two arrows pointing to the browser's address bar and the registration form below.
- 3rd Party:** A red box on the right with an arrow pointing to a Bitdefender advertisement.

**Browser Address Bar:** nytimes.com

**Page Header:** The New York Times, POLITICS, LOG IN

**Advertisement:** Bitdefender. Global Leader. In Cybersecurity. Keep your data truly safe. GET 6 MONTHS FREE.

**Registration Form:**

**Create a free account, or log in.**

Gain access to limited free articles, news alerts, select newsletters, podcasts and some daily games.

Email Address

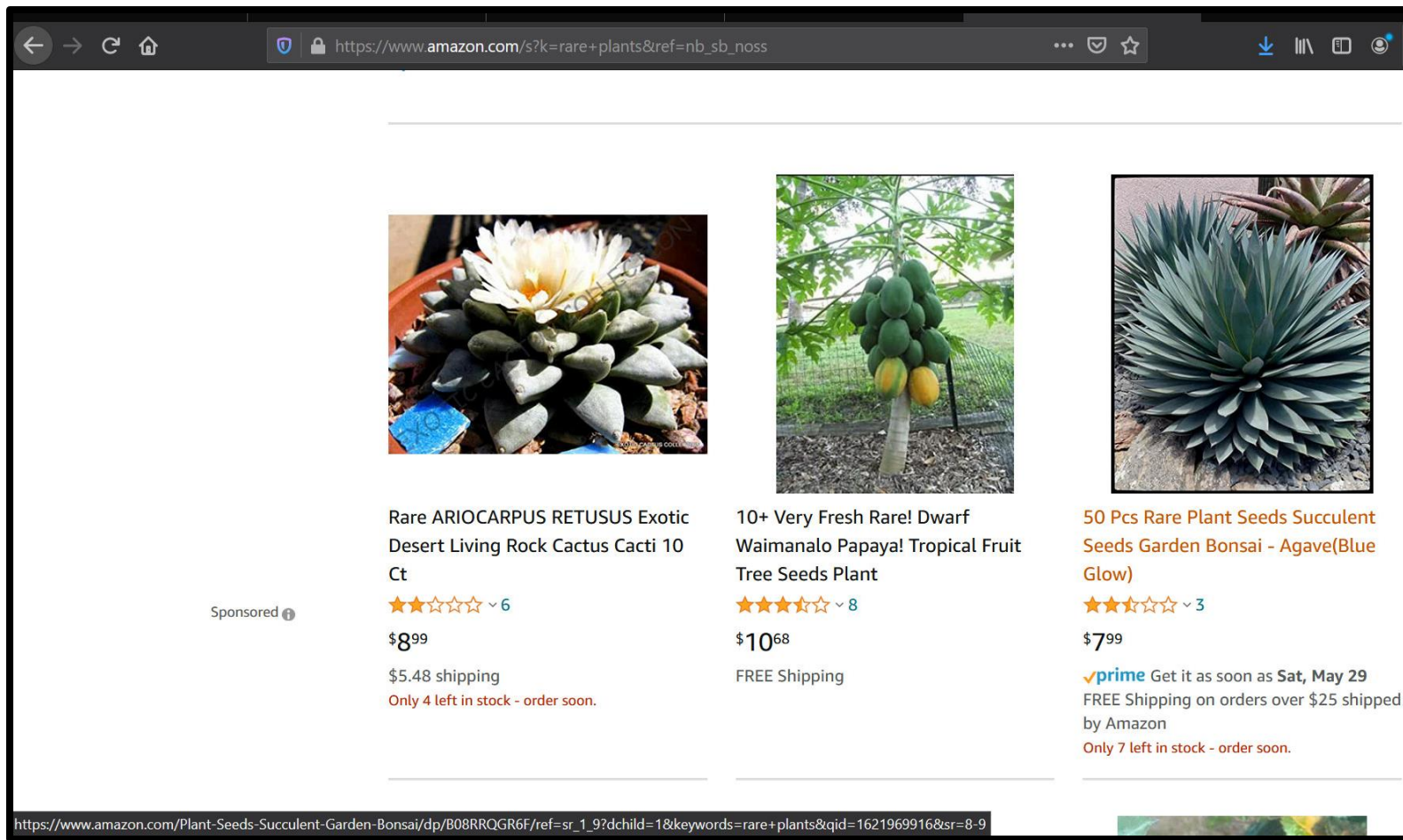
Continue

or

By continuing you agree to our Terms of Service and Privacy Policy

# Mechanics of First-Party Online Tracking

- Use cookies, JavaScript, URL parameters to track



# Mechanics of First-Party Online Tracking

<p>Sponsored ⓘ</p>	<p>Desert Living Rock Cactus Cacti 10 Ct</p> <p>★★★★☆ ∨ 6</p> <p>\$8<sup>99</sup></p> <p>\$5.48 shipping</p> <p>Only 4 left in stock - order soon.</p>	<p>Waimanalo Papaya! Tropical Fruit Tree Seeds Plant</p> <p>★★★★☆ ∨ 8</p> <p>\$10<sup>68</sup></p> <p>FREE Shipping</p>	<p>Seed Glow</p> <p>★★★</p> <p>\$7<sup>99</sup></p> <p>✓prime</p> <p>FREE by An</p> <p>Only 7</p>
<p><a href="https://www.amazon.com/Plant-Seeds-Succulent-Garden-Bonsai/dp/B08RRQGR6F/ref=sr_1_9?dchild=1&amp;keywords=rare+plants&amp;qid=1621969916&amp;sr=8-9">https://www.amazon.com/Plant-Seeds-Succulent-Garden-Bonsai/dp/B08RRQGR6F/ref=sr_1_9?dchild=1&amp;keywords=rare+plants&amp;qid=1621969916&amp;sr=8-9</a></p>			

# Mechanics of Third-Party Online Tracking

The screenshot displays the UChicago News website. At the top, the browser address bar shows 'https://www.uchicago.edu' with a 67% zoom level. The main heading is 'UChicago News', followed by a sub-header: '- Visit the UChicago Forward website, for the University's COVID-19 health protocols, campus guidelines, and other Spring Quarter information.'

Below the header, there are three featured news items, each with a thumbnail image and a title:

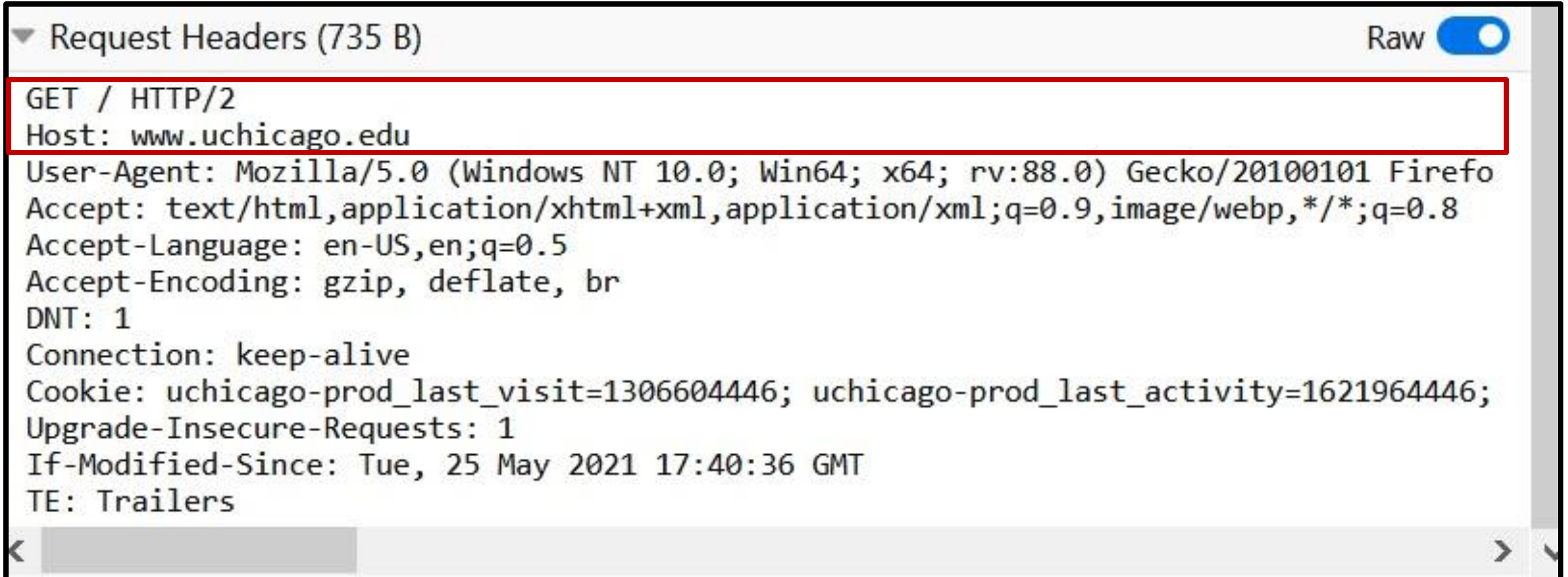
- What Americans are thinking a year after George Floyd's death**: The thumbnail shows a street scene with many people and flowers.
- Big Brains podcast: Why You're Likely Paying An Unfair Share of Property Taxes**: The thumbnail shows a row of small, stylized houses.
- University announces COVID-19 vaccine requirement for all students**: The thumbnail shows a modern building with a large tree in the foreground.

To the right of these items is a section titled 'Latest News' with the text: 'Founded at UChicago, nonprofit Climate Vault proposes new solution for carbon reduction'. A 'MORE NEWS >' link is located at the bottom right of this section.

At the bottom of the page, there is a video player for a video titled 'Explore Chicago: Discover the Global City UChicago...'. The video player has a red border and includes a play button, a 'Watch later' button, and a 'Share' button. The video content shows a street scene with a large building and people walking. Below the video player is a 'Watch on YouTube' button. To the right of the video player is a section titled 'Explore Chicago' with the text: 'Discover the global city UChicago calls home—filled with inspiration, innovation, and countless opportunities to explore.' and a 'VISIT UCHICAGO >' link.

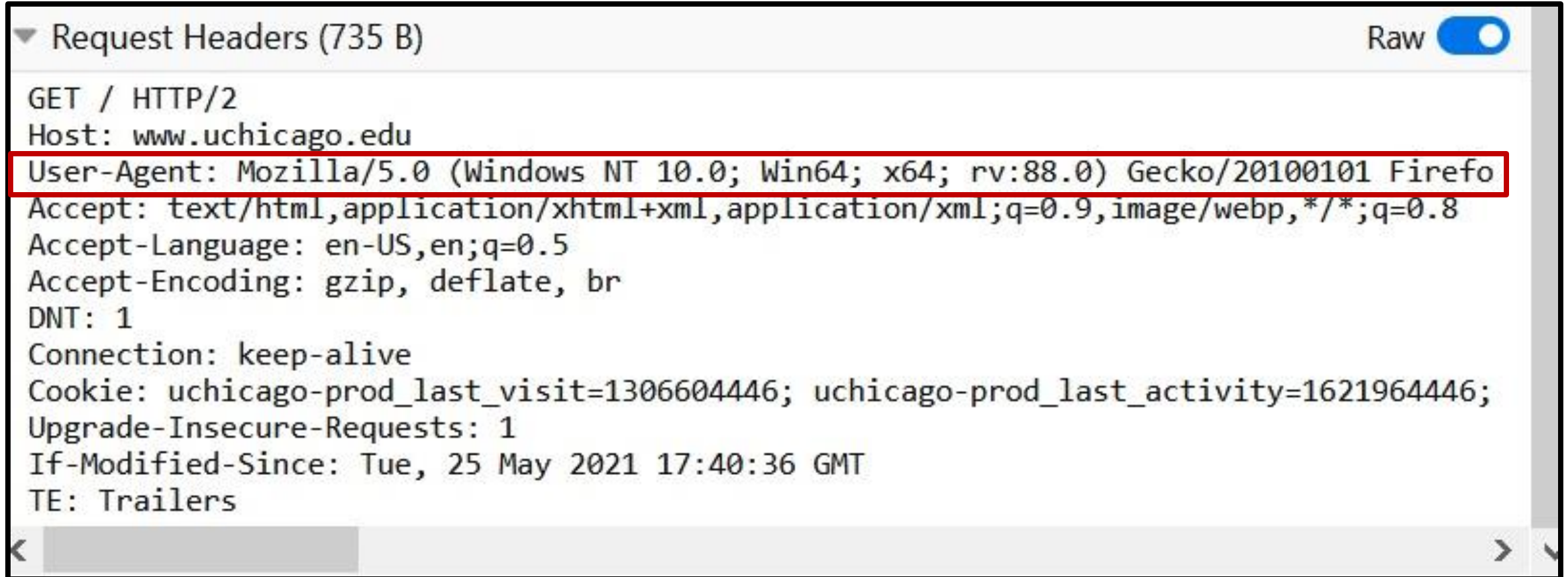



# Details of What's Happening in HTTP (Request)



```
▼ Request Headers (735 B) Raw ☒  
GET / HTTP/2  
Host: www.uchicago.edu  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefo  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate, br  
DNT: 1  
Connection: keep-alive  
Cookie: uchicago-prod_last_visit=1306604446; uchicago-prod_last_activity=1621964446;  
Upgrade-Insecure-Requests: 1  
If-Modified-Since: Tue, 25 May 2021 17:40:36 GMT  
TE: Trailers
```

# Details of What's Happening in HTTP (Request)



```
▼ Request Headers (735 B) Raw   
GET / HTTP/2  
Host: www.uchicago.edu  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefo  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate, br  
DNT: 1  
Connection: keep-alive  
Cookie: uchicago-prod_last_visit=1306604446; uchicago-prod_last_activity=1621964446;  
Upgrade-Insecure-Requests: 1  
If-Modified-Since: Tue, 25 May 2021 17:40:36 GMT  
TE: Trailers
```

# Details of What's Happening in HTTP (Request)

▼ Request Headers (735 B) Raw ☒

GET / HTTP/2  
Host: www.uchicago.edu  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefo  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate, br  
DNT: 1  
Connection: keep-alive  
Cookie: uchicago-prod\_last\_visit=1306604446; uchicago-prod\_last\_activity=1621964446;  
Upgrade-Insecure-Requests: 1  
If-Modified-Since: Tue, 25 May 2021 17:40:36 GMT  
TE: Trailers

<  >

# Details of What's Happening in HTTP (Cookies)



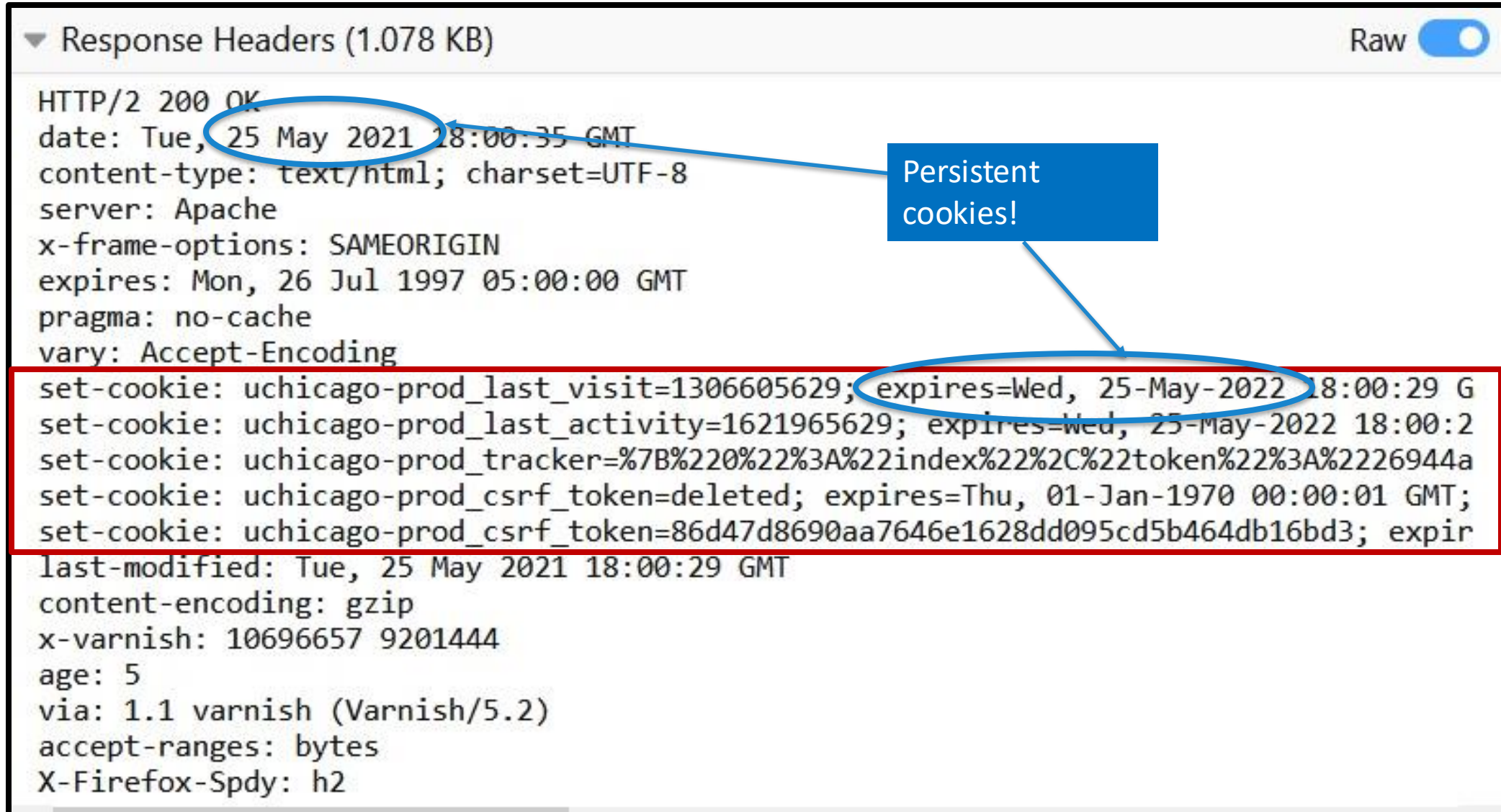


# Details of What's Happening in HTTP (Response)

▼ Response Headers (1.078 KB) Raw ☒

```
HTTP/2 200 OK
date: Tue, 25 May 2021 18:00:35 GMT
content-type: text/html; charset=UTF-8
server: Apache
x-frame-options: SAMEORIGIN
expires: Mon, 26 Jul 1997 05:00:00 GMT
pragma: no-cache
vary: Accept-Encoding
set-cookie: uchicago-prod_last_visit=1306605629; expires=Wed, 25-May-2022 18:00:29 G
set-cookie: uchicago-prod_last_activity=1621965629; expires=Wed, 25-May-2022 18:00:2
set-cookie: uchicago-prod_tracker=%7B%220%22%3A%22index%22%2C%22token%22%3A%2226944a
set-cookie: uchicago-prod_csrf_token=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT;
set-cookie: uchicago-prod_csrf_token=86d47d8690aa7646e1628dd095cd5b464db16bd3; expir
last-modified: Tue, 25 May 2021 18:00:29 GMT
content-encoding: gzip
x-varnish: 10696657 9201444
age: 5
via: 1.1 varnish (Varnish/5.2)
accept-ranges: bytes
X-Firefox-Spdy: h2
```

# Details of What's Happening in HTTP (Response)



## UChicago News

- Visit the [UChicago Forward website](#), for the University's COVID-19 health protocols, campus guidelines, and other Spring Quarter information.



What Americans are thinking a year after George Floyd's death



Big Brains podcast: Why You're Likely Paying An Unfair Share of Property Taxes



University announces COVID-19 vaccine requirement for all students

### Latest News

Founded at UChicago, nonprofit Climate Vault proposes new solution for carbon reduction

[MORE NEWS >](#)



Explore Chicago: Discover the Global City UChicag...



Watch later



Share

# A WORLD-CLASS UNIVERSITY

Watch on  YouTube

## Explore Chicago

Discover the global city UChicago calls home—filled with inspiration, innovation, and countless opportunities to explore.

[VISIT UCHICAGO >](#)



# HTTP Headers (uchicago.edu → youtube.com)

The screenshot displays the Chrome DevTools Network tab with the 'Headers' sub-tab selected. The left pane shows a list of network requests, with the third request (a GET to a YouTube video embed) highlighted. The right pane shows the details of this request, including status, version, and various headers.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.uchicago.edu	/	document	html	11.41 KB	39...
204	POST	www.youtube.com	atr?ns=yt&el=embedded&cpn=ho5PKBh-	base.js:1023 (...)	html	604 B	0 B
200	GET	www.youtube.com	P-xlixF7B2U?autoplay=1&fs=1&autohide=1&subdocument	subdocument	html	21.81 KB	51...
200	GET	cdn.hypemarmarketing.com	uchicagowww?width=1169&paginate=tru	a5b5e5.js:3 (s...	html	128.06 KB	12...
200	GET	cdn.hypemarmarketing.com	popUpModalEndpoint	a5b5e5.js:3 (s...	html	10.99 KB	10...

**Request Headers (621 B)**

```
GET /embed/P-xlixF7B2U?autohide=1&fs=1&autoplay=0&rel=0&modestbranding=1&showinfo=0&hd=1&Host: www.youtube.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Alt-Used: www.youtube.com
Connection: keep-alive
Referer: https://www.uchicago.edu/
Cookie: VISITOR_INFO1_LIVE=dActKPaJViQ; PREF=tz=America.Chicago&f4=4000000; YSC=p2jSvxCMelI
Upgrade-Insecure-Requests: 1
TE: Trailers
```

**Response Headers (642 B)**

```
HTTP/3 200 OK
content-type: text/html; charset=utf-8
x-content-type-options: nosniff
cache-control: no-cache, no-store, max-age=0, must-revalidate
pragma: no-cache
expires: Mon, 01 Jan 1990 00:00:00 GMT
date: Tue, 25 May 2021 18:00:36 GMT
strict-transport-security: max-age=31536000
permissions-policy: ch-ua-full-version=*, ch-ua-platform=*, ch-ua-platform-version=*, ch-ua-content-encoding: br
server: ESF
x-xss-protection: 0
alt-svc: h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000
```

5 requests | 229.65 KB / 172.86 KB transferred | Finish: 4.03 min | DOMContentLoaded: 451 ms | load: 1.70 s

# HTTP Headers (uchicago.edu → youtube.com)

Status	Met...	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.uchica...	/	document	html	11.41 KB	39...
204	POST	www.youtub...	atr?ns=yt&el=embedded&cpn=ho5PKBh-	base.js:1023 (...)	html	604 B	0 B
200	GET	www.youtub...	P-xlixF7B2U?autohide=1&fs=1&autoplay=	subdocument	html	21.81 KB	51...
200	GET	cdn.hypemar...	uchicagowww?width=1169&paginate=tru	a5b5e5.js:3 (s...	html	128.06 KB	12...
200	GET	cdn.hypemar...	popUpModalEndpoint	a5b5e5.js:3 (s...	html	10.99 KB	10...

# HTTP Headers (uchicago.edu → youtube.com)

## ▼ Request Headers (621 B)

Raw 

```
GET /embed/P-xlixF7B2U?autohide=1&fs=1&autoplay=0&rel=0&modestbranding=1&showinfo=0&hd=1&e
Host: www.youtube.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Alt-Used: www.youtube.com
Connection: keep-alive
Referer: https://www.uchicago.edu/
Cookie: VISITOR_INFO01_LIVE=dACtKPaJViQ; PREF=tz=America.Chicago&f4=4000000; YSC=p2jSvxCMel
Upgrade-Insecure-Requests: 1
TE: Trailers
```



# HTTP Headers (uchicago.edu → youtube.com)

## ▼ Request Headers (621 B)

Raw 

```
GET /embed/P-xlixF7B2U?autohide=1&fs=1&autoplay=0&rel=0&modestbranding=1&showinfo=0&hd=1&e
Host: www.youtube.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Alt-Used: www.youtube.com
Connection: keep-alive
Referer: https://www.uchicago.edu/
Cookie: VISITOR_INFO01_LIVE=dACtKPaJViQ; PREF=tz=America.Chicago&f4=4000000; YSC=p2jSvxCMel
Upgrade-Insecure-Requests: 1
TE: Trailers
```

# Putting It Together: Simple 3<sup>rd</sup> Party Tracking

- (Unless browser blocks it) third party gets its cookies
- (Unless browser blocks it) third party sees “referrer” [sic]
- 1<sup>st</sup> party can choose to send info to third party via URL parameters (not a violation of Same Origin Policy!)
- 3<sup>rd</sup> party sees this information for **many** first parties (whoever embeds them!)
- In practice, advertising & 3<sup>rd</sup> party tracking much more complicated (lots of different 3<sup>rd</sup> parties involved)



# Alternatives to Cookies for Tracking / Profiling

# Various Side Channels

- **Side channel:** learning information through indirect means
- (Loophole has since mostly been closed)

```
a:visited {  
    color: purple;  
}
```

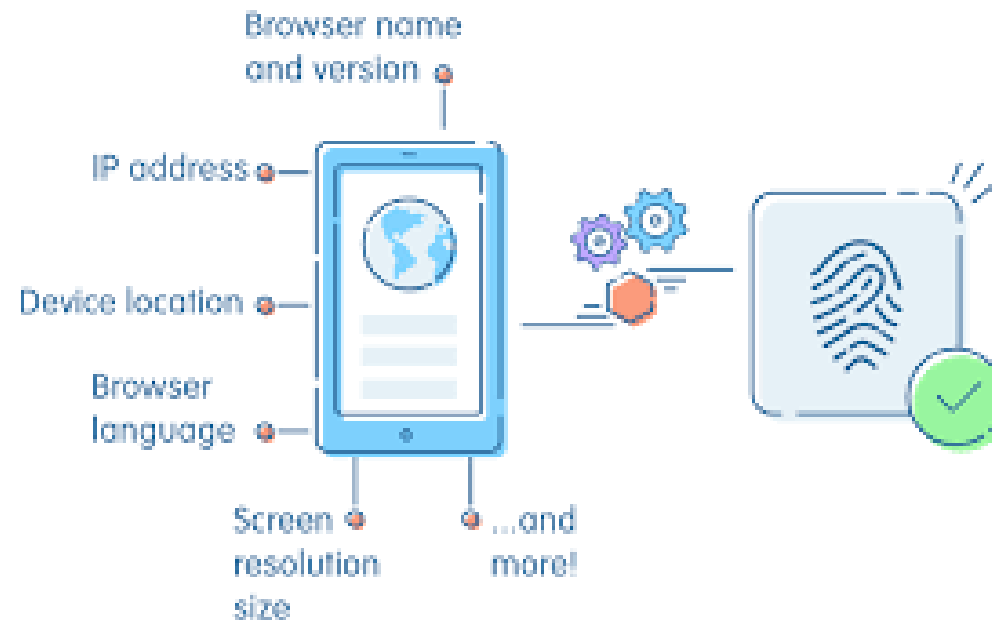
- link one
- second link
- link three (visited)
- fourth link

# Browser Fingerprinting

- Use features of the browser that are relatively unique to your machine
  - Fonts
  - GPU model anti-aliasing (Canvas fingerprinting)
  - User-agent string
  - *(Often not)* IP address *(Why not?)*

# Browser Fingerprinting

- Use combination of device features as an identifier
- <https://coveryourtracks.eff.org/>



# Various Legal & Regulatory Efforts

- GDP
- Ne
- pa

YOUR LOGO

Powered by **Cookiebot**  
by Usercentrics

Consent

Details

About

**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Necessary

Preferences

Statistics

Marketing

Deny

Allow Selection

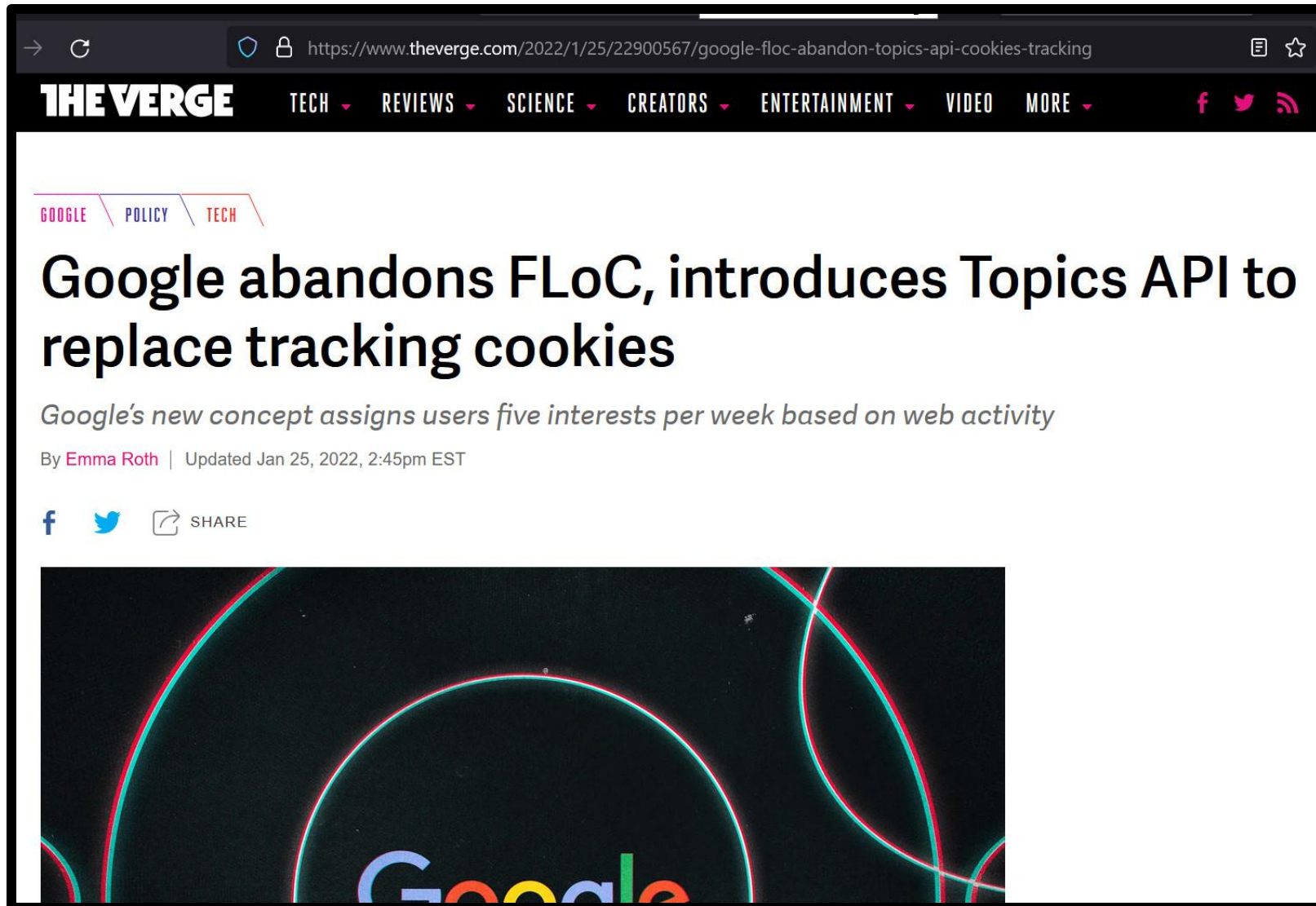
Allow all

for 3<sup>rd</sup>

# Various Legal & Regulatory Efforts

- GDPR (EU) & CCPA (California)
  - New laws to require explicit opt-in consent & transparency for 3<sup>rd</sup> party cookie use & tracking mechanisms
- Google originally aimed to completely phase out 3<sup>rd</sup> party cookies from the web by 2025 (unclear status now)

# Google's Topics API



# Google's Topics API

