

User Awareness and Behaviors Concerning Encrypted DNS Settings in Web Browsers

Alexandra Nisenoff, **Ranya Sharma**, Nick Feamster



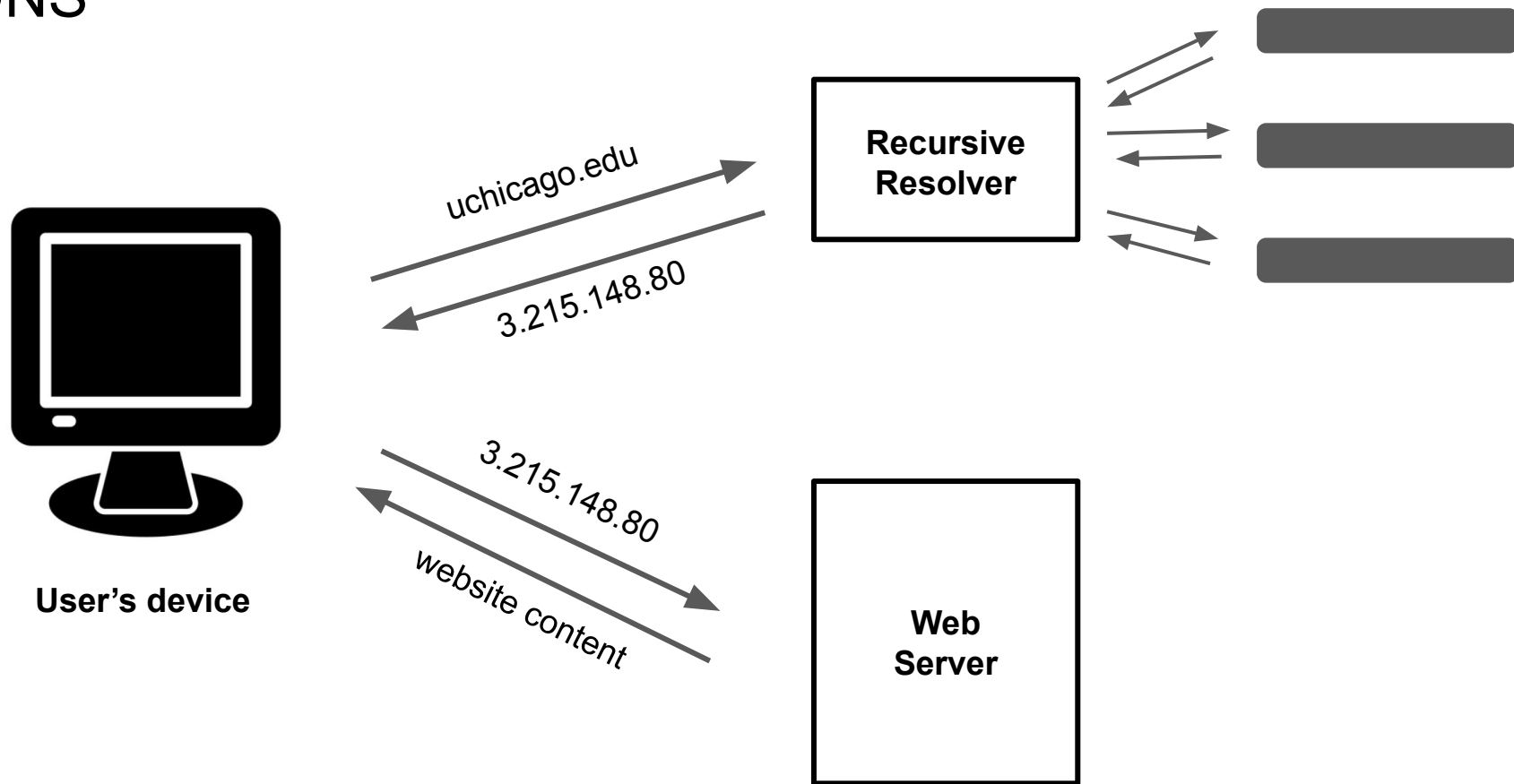
THE UNIVERSITY OF
CHICAGO

Carnegie Mellon University

Motivation

- Current encrypted DNS ecosystem has a power imbalance
 - Interferes with technical design
- Design choices affect
 - Market consolidation
 - User privacy
 - User experience

DNS



Our Study

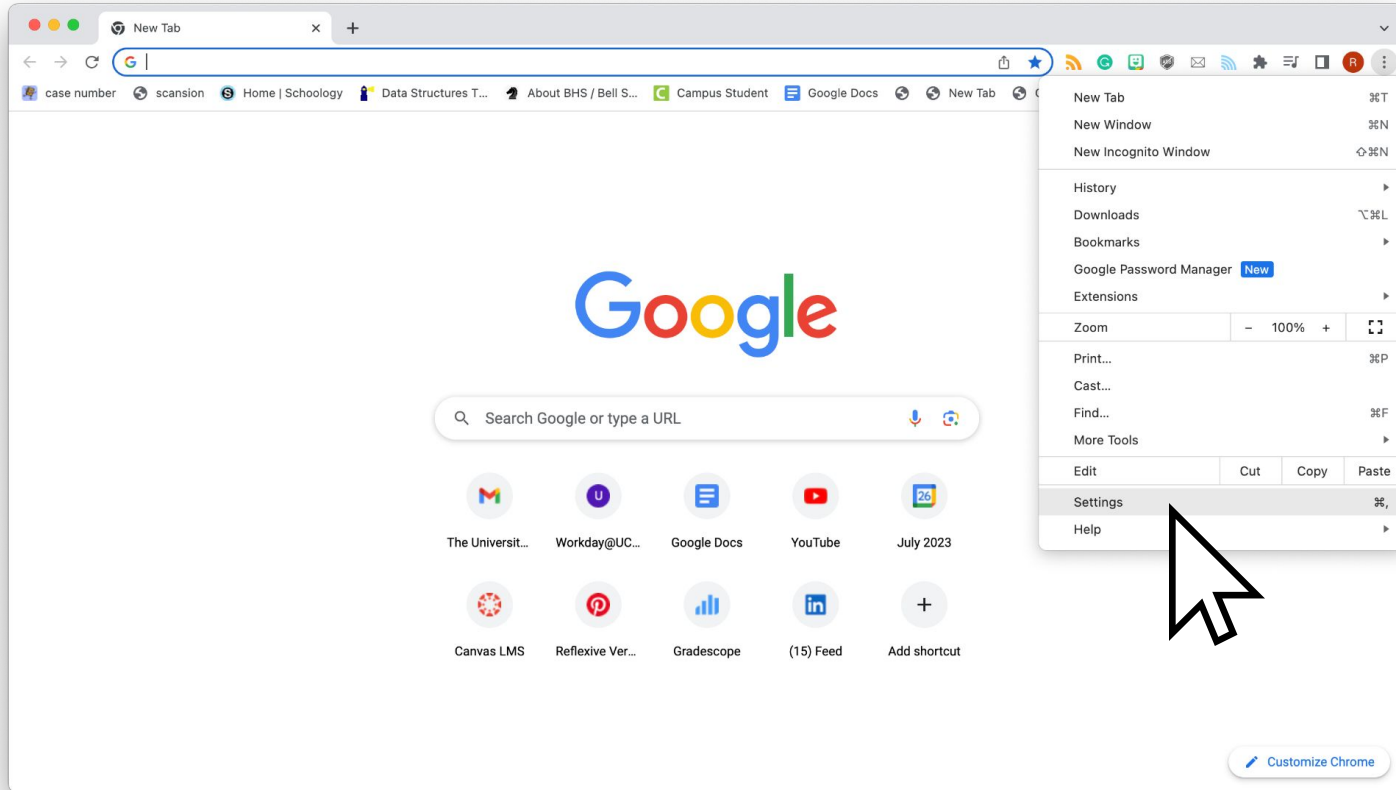
Browsers



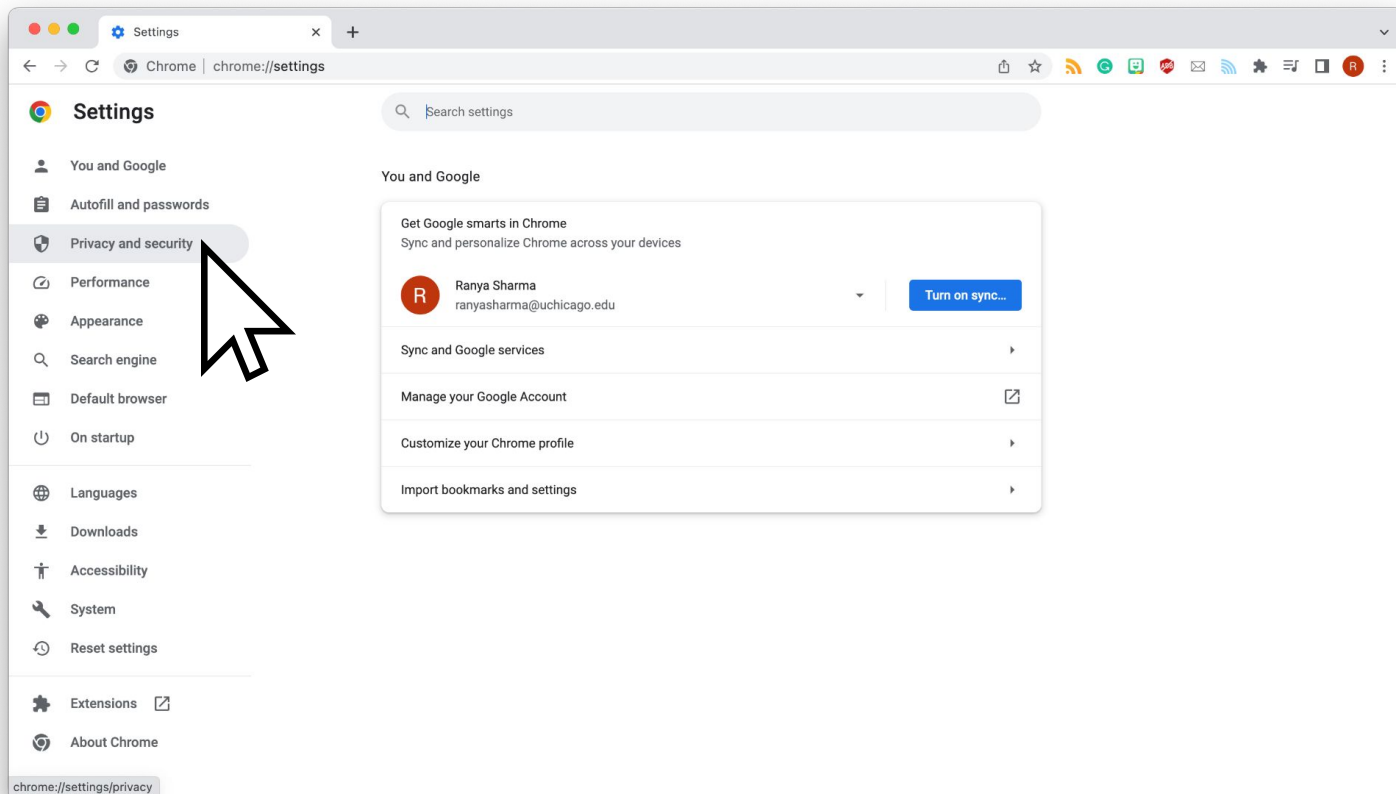
Mobile Operating Systems



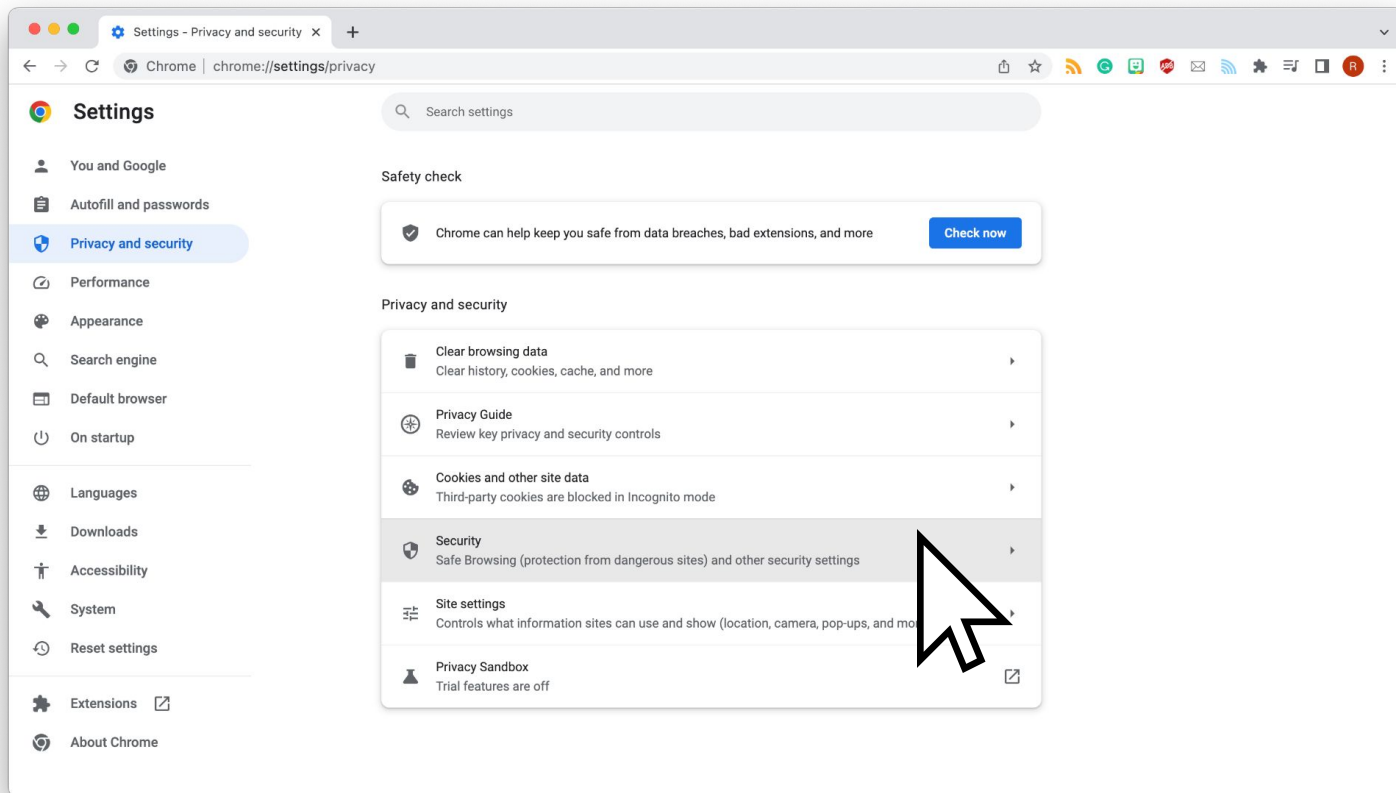
Encrypted DNS in Chrome



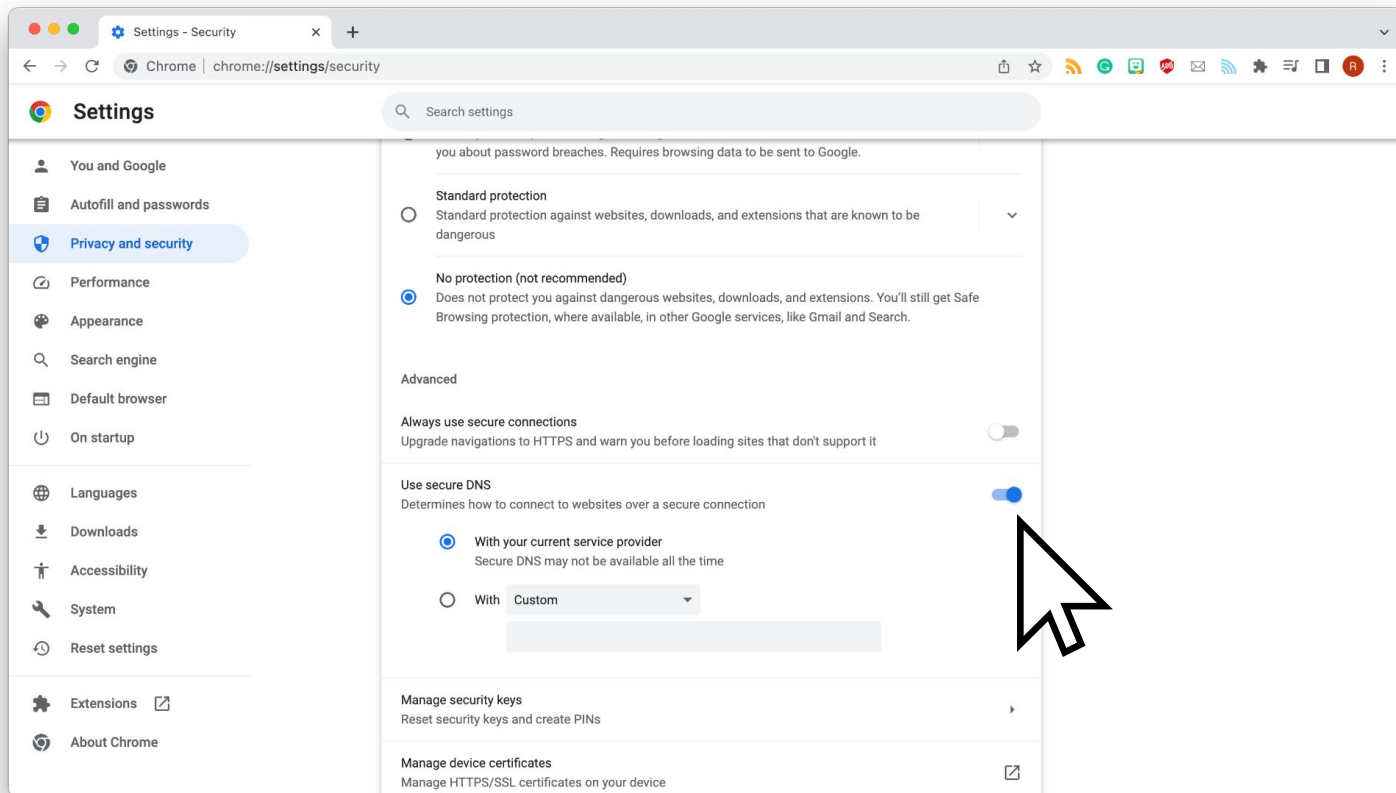
Encrypted DNS in Chrome



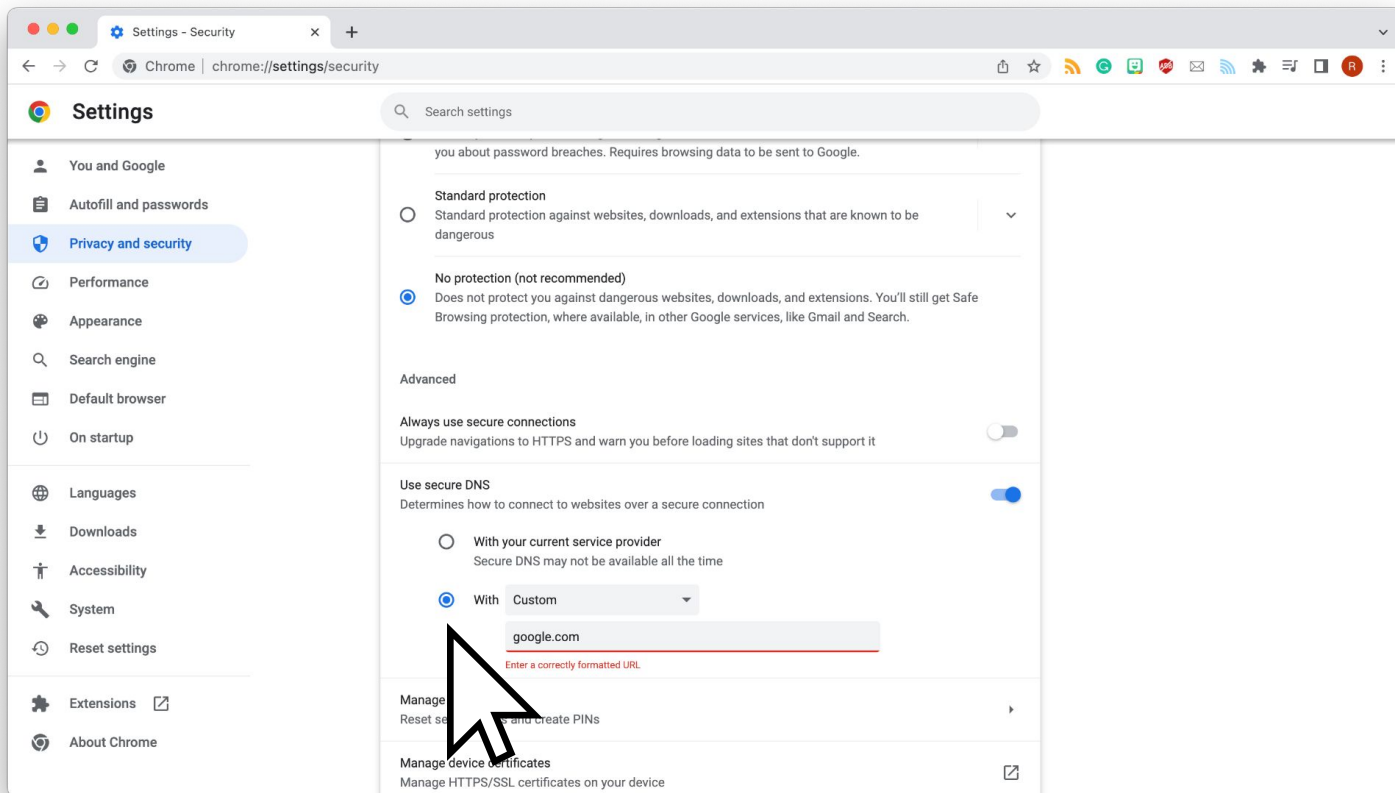
Encrypted DNS in Chrome



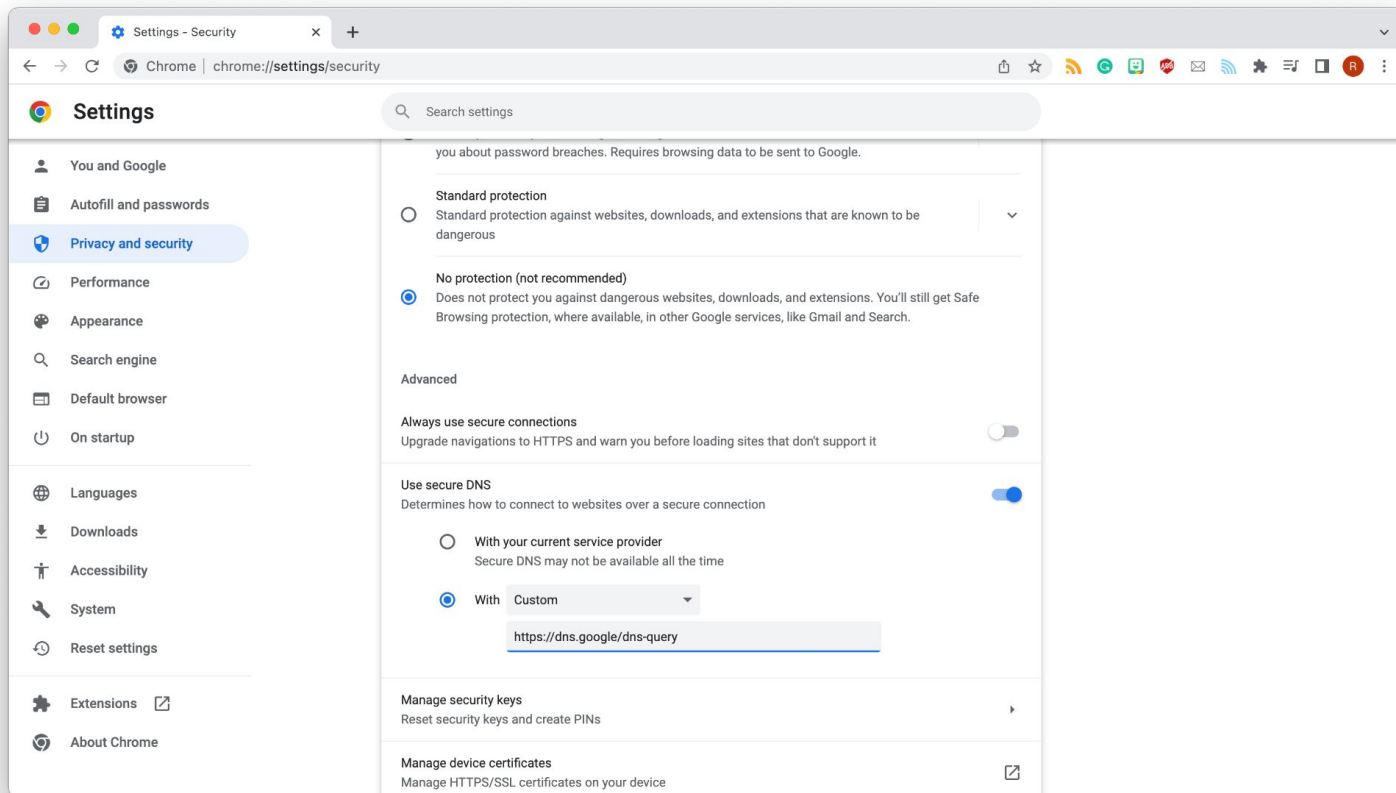
Encrypted DNS in Chrome



Encrypted DNS in Chrome



Encrypted DNS in Chrome



Enabling DNS-over-HTTPS

Use secure DNS 

Determines how to connect to websites over a secure connection

☒ With your current service provider
Secure DNS may not be available all the time

☐ With

See this provider's [privacy policy](#)



Use secure DNS 

Determines how to connect to websites over a secure connection

☒ With your current service provider
Secure DNS may not be available all the time

☐ With



Use secure DNS to specify how to lookup the network address for websites 

By default, Microsoft Edge uses your current service provider. Alternate DNS providers may cause some sites to not be reachable.

☐ Use current service provider
Your current service provider may not provide secure DNS

☐ Choose a service provider
Select a provider from the list or enter a custom provider



☐ Do not prompt for authentication if password is saved

☐ Proxy DNS when using SOCKS v5

☒ Enable DNS over HTTPS

Use Provider



Use DNS-over-HTTPS instead of the system's DNS settings 

This functionality uses third party services. Please read our [Terms of Use](#) and [Privacy Policy](#) to learn more.

DNS-over-HTTPS provider:

☒ Cloudflare (default)

☐ Cloudflare for Families (No Malware)

☐ Cloudflare for Families (No Malware or Adult Content)

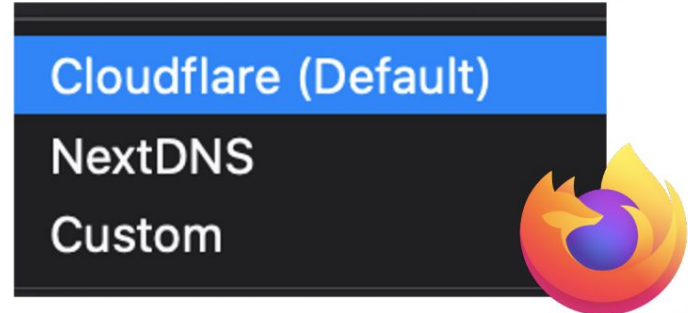
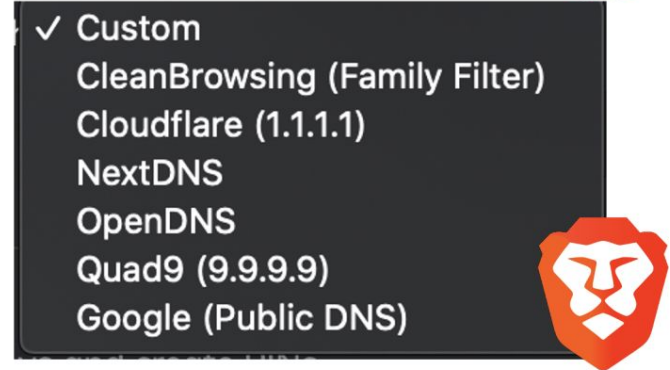
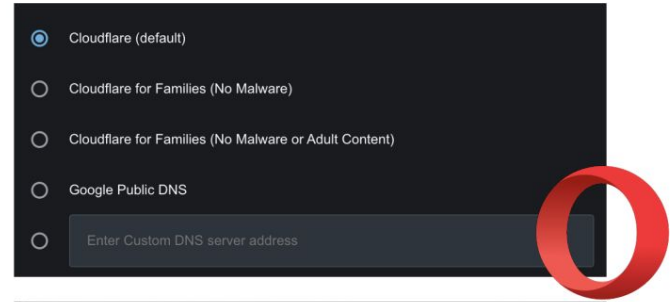
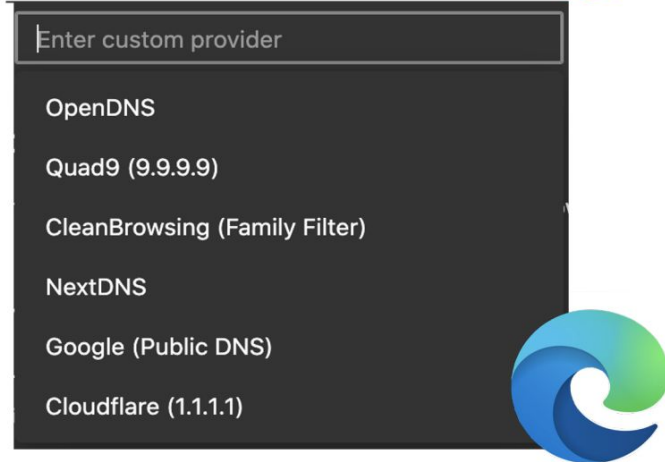
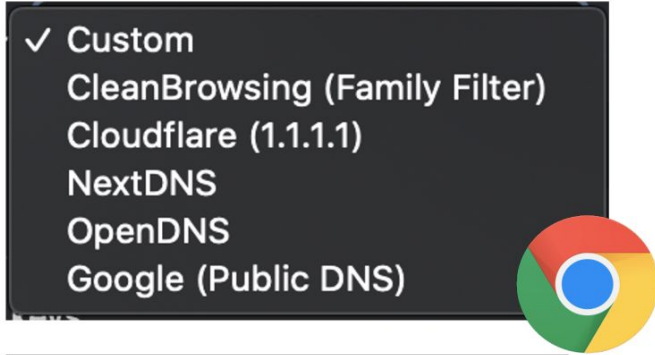
☐ Google Public DNS

☐

eg. <https://opera.cloudflare-dns.com/dns-query>



Choosing a Trusted Resolver



Research Questions

1. Are users **aware** of encrypted DNS settings in browsers and devices?
2. What encrypted DNS settings do users have **enabled**?
3. When **shown** encrypted DNS **settings** for different browsers, **which** settings **do users select**?
4. When the **technical aspects** of these systems are **explained** to users, how do their choices of settings **change**?

Our Study Methods

Screening Survey

Main Survey

Our Study Methods

Screening Survey

Browser usage

800 participants

Main Survey

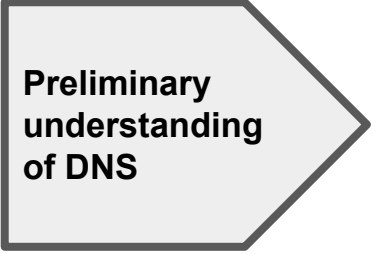
Our Study Methods

Screening Survey

Main Survey

- 184 participants
- Participants assigned to subgroups
- Up to 50 participants from each subgroup participate in main survey

Main Survey



**Preliminary
understanding
of DNS**

Main Survey

Preliminary
understanding
of DNS

Interactive
versions
of
browsers



n = 45



n = 51

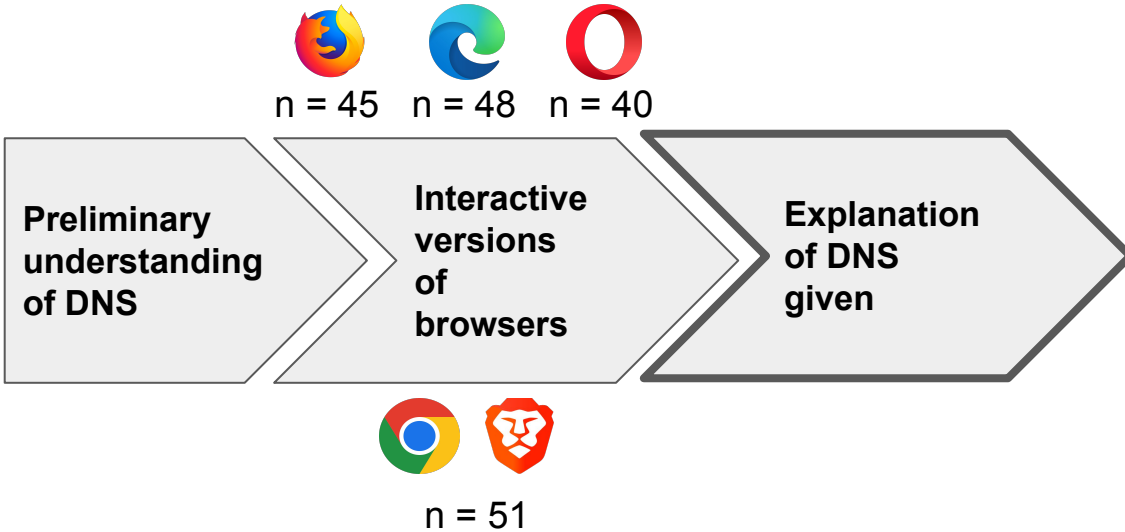


n = 48

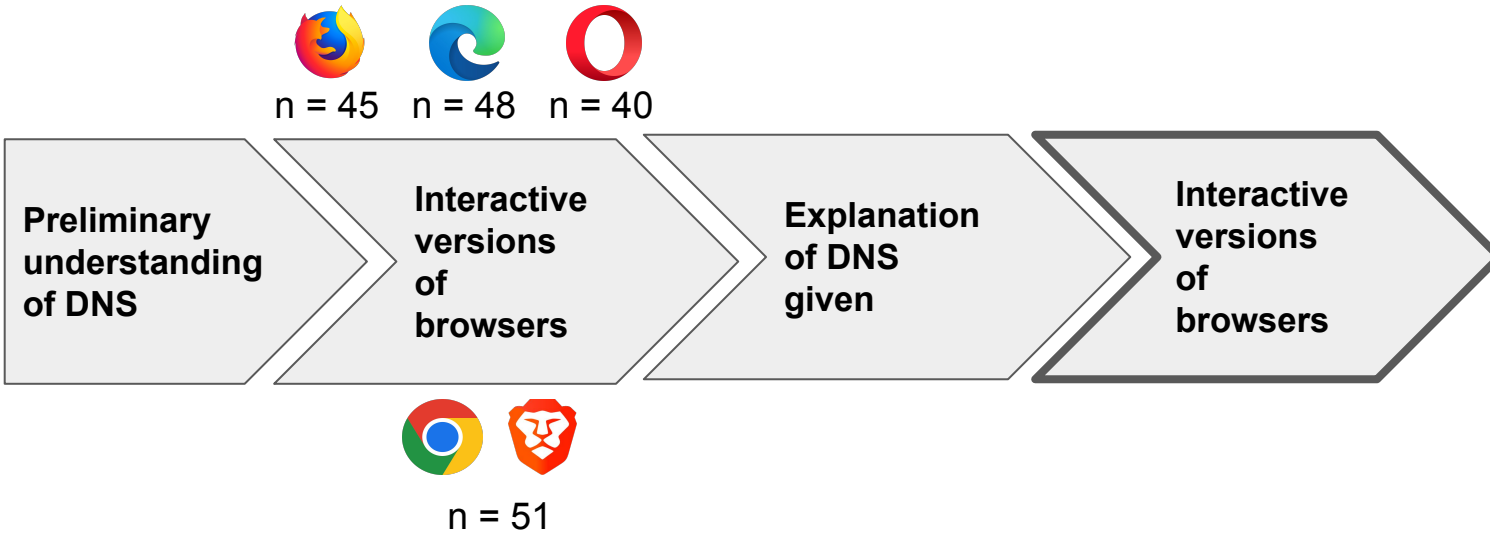


n = 40

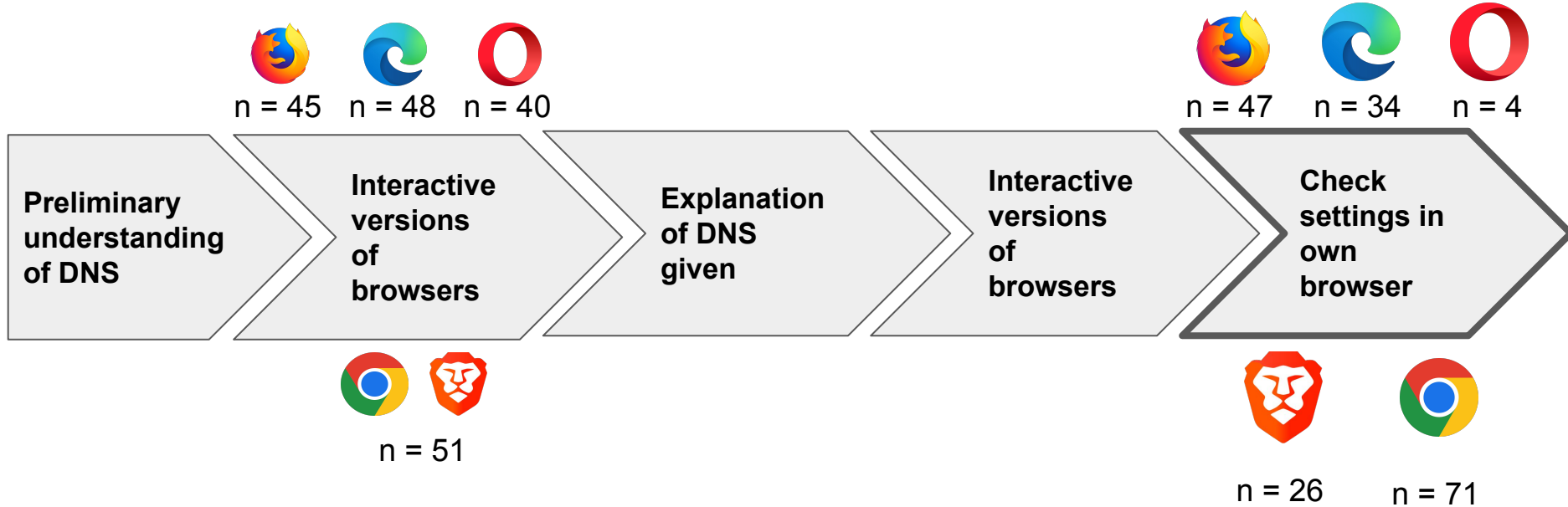
Main Survey



Main Survey

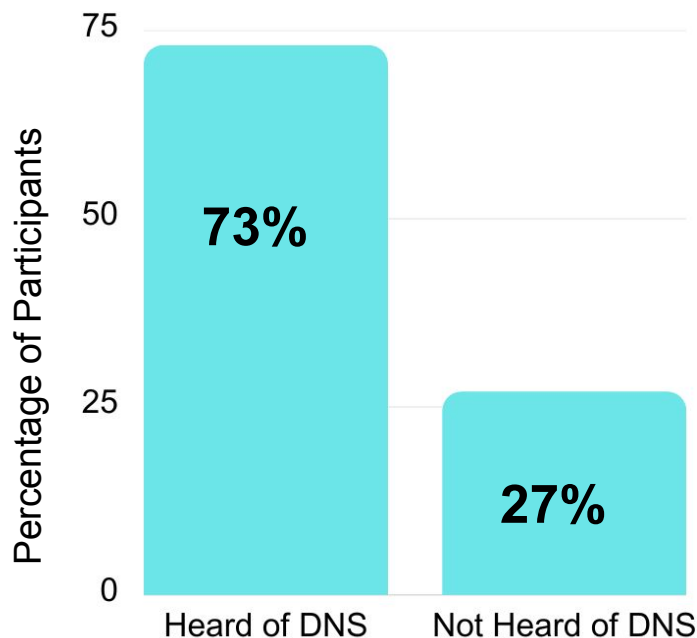


Main Survey

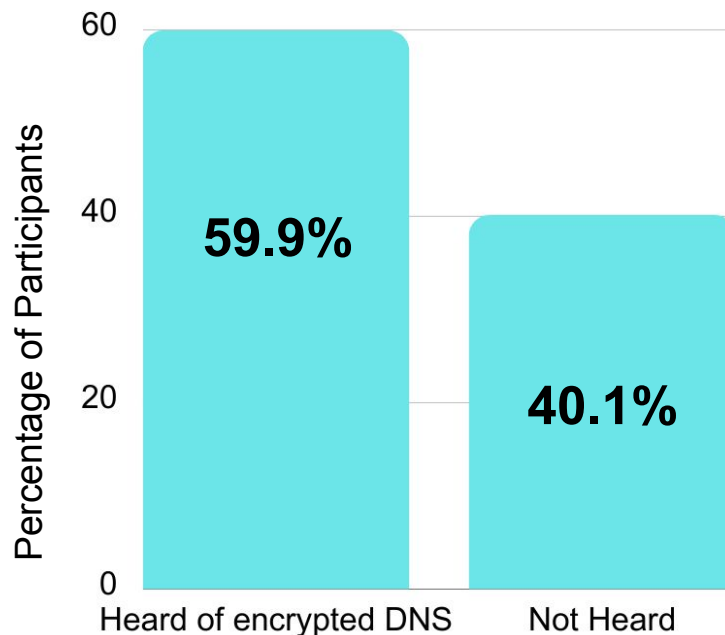


Are users aware of encrypted DNS settings?

High percentage of participants reported **having heard of DNS** prior to the survey

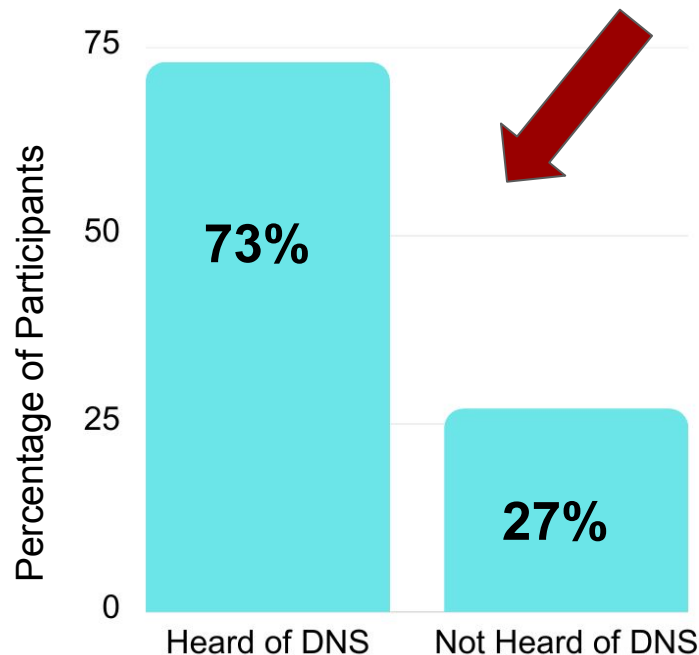


Of the participants who reported **having heard of DNS**, more than half had heard of **encrypted DNS**.

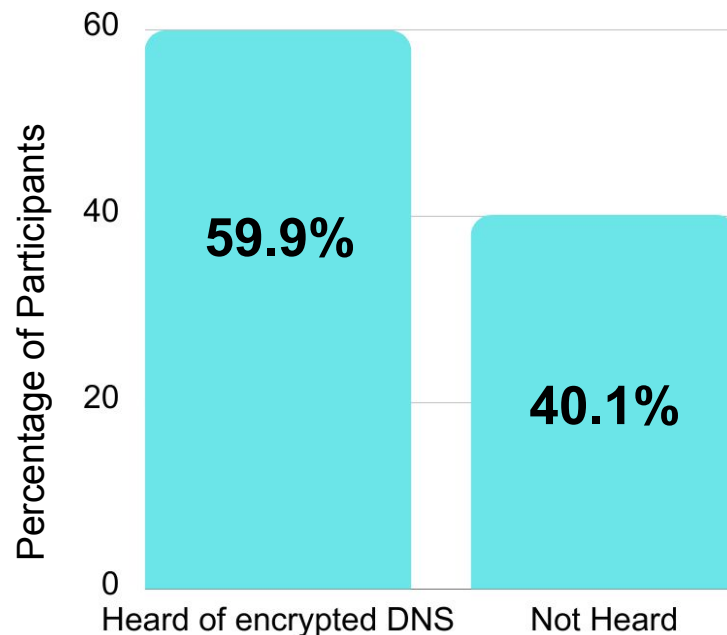


Are users aware of encrypted DNS settings?

High percentage of participants reported **having heard of DNS** prior to the survey

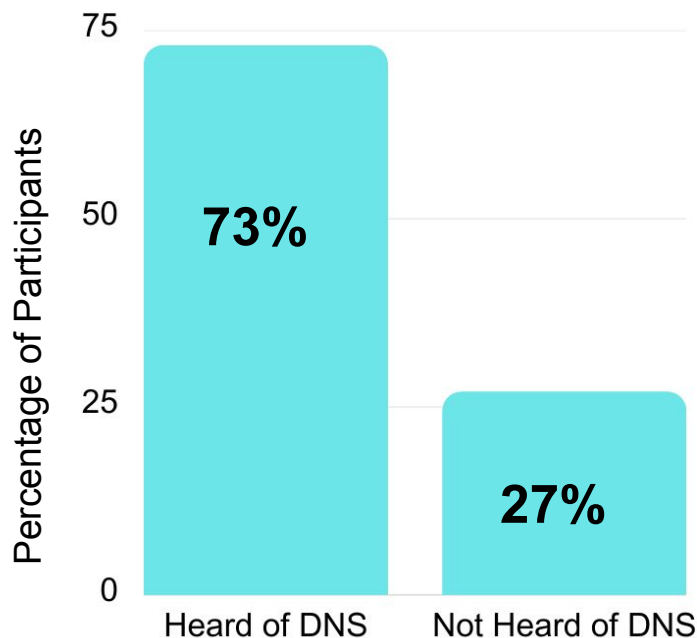


Of the participants who reported **having heard of DNS**, more than half had heard of **encrypted DNS**.

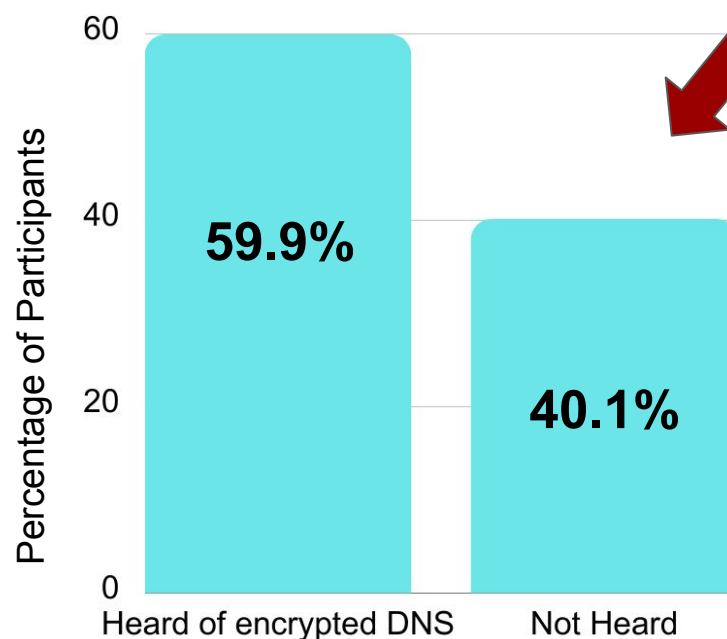


Are users aware of encrypted DNS settings?

High percentage of participants reported **having heard of DNS** prior to the survey

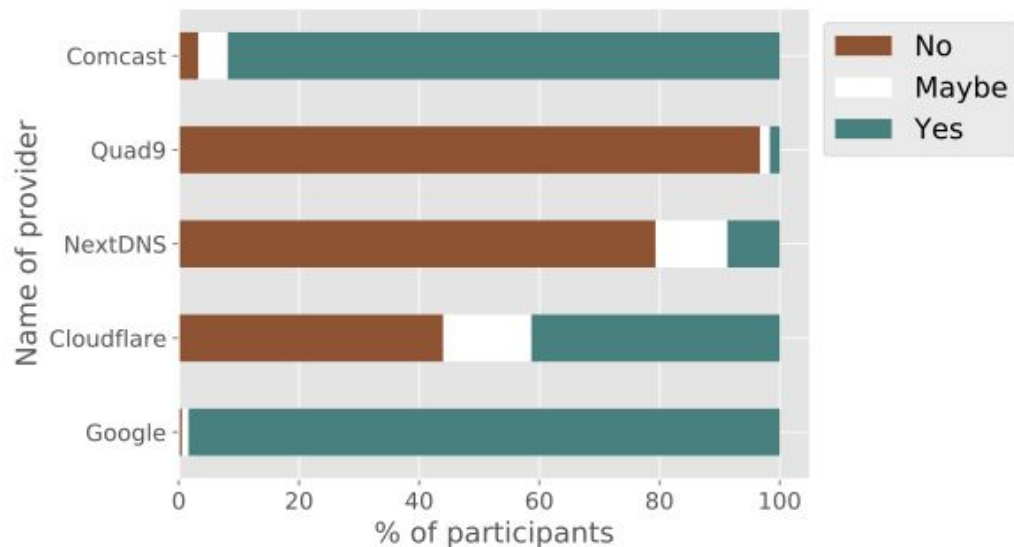


Of the participants who reported **having heard of DNS**, more than half had heard of **encrypted DNS**.



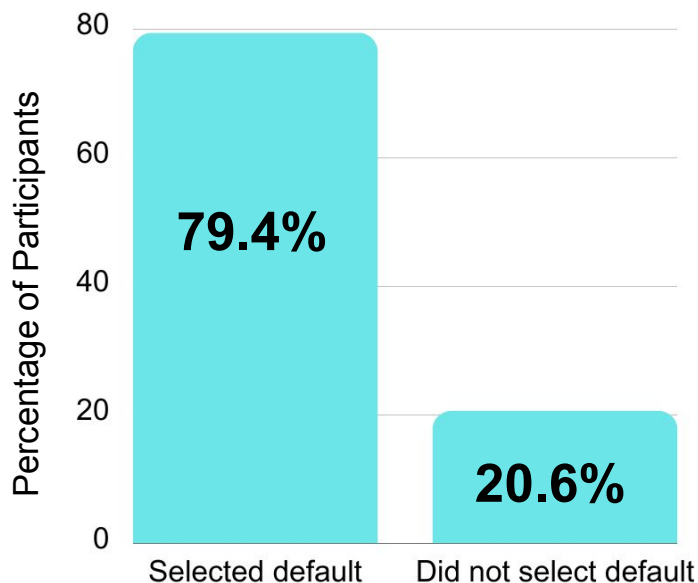
Are users aware of encrypted DNS settings?

Comcast and Google were widely known providers, while NextDNS and Quad9 were scarcely heard of



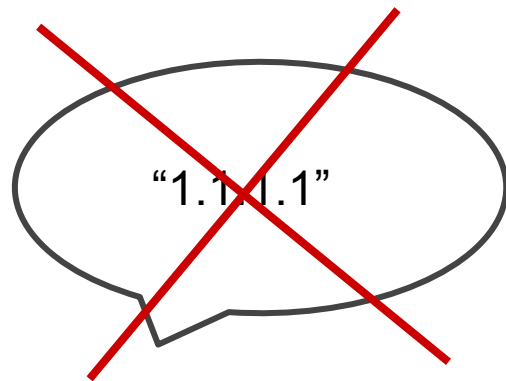
What encrypted DNS settings do users have enabled?

Most participants selected the default settings in their browsers



No participants correctly configured a custom DNS resolver in their browser.

Custom Resolvers

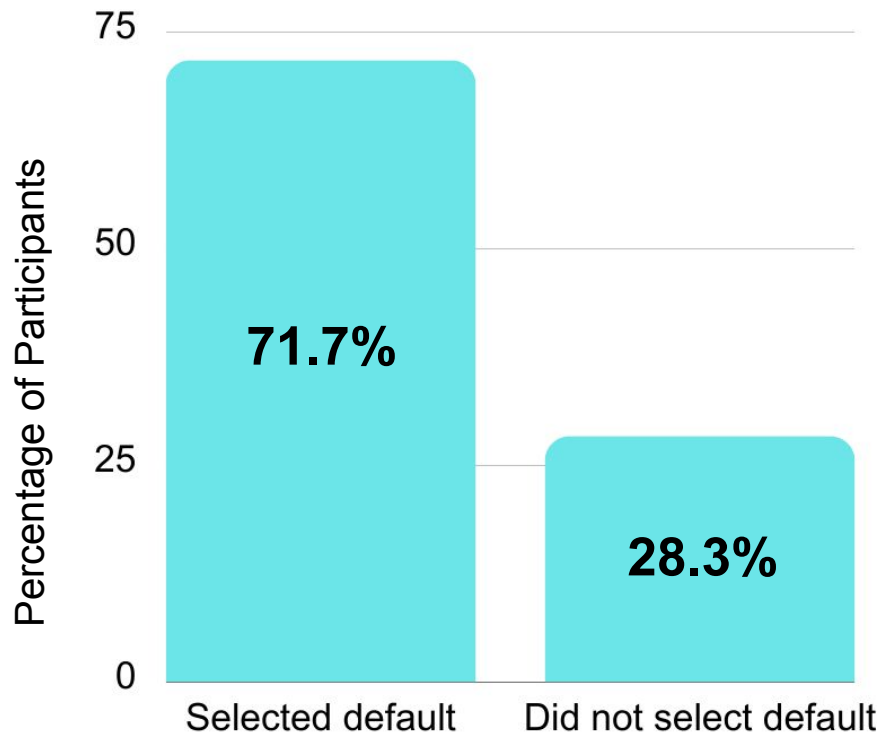


<https://dns.google/dns-query>

<https://dns.cloudflare.com/dns-query>

When shown encrypted DNS settings for different browsers, which settings do users select?

Most participants continued to use the default settings shown to them



When shown encrypted DNS settings for different browsers, which settings do users select?

Name of setting and perceived impact

- “Secure DNS”
- “DNS-over-HTTPS”

Participants associated Secure DNS with **safety** and **security**.

“The wording makes it sound like enabling DNS would make my browser more secure,” (P6).

“I don't know a lot about it but it seems like an extra step of protection,” (P50).

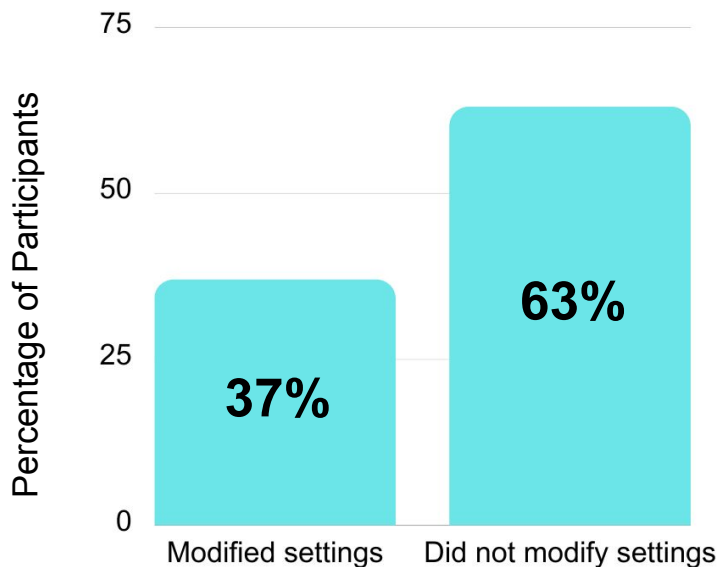
Instead of interpreting DNS-over-HTTPS as meaning **DNS *using* the HTTPS** protocol, they interpreted DoH as meaning use **DNS *instead* of HTTPS**

“I have no earthly idea what DNS is, while I at least have a passing familiarity with HTTPS,” (P3).

“From the little I know I believe that HTTPS is more secure than DNS,” (P30).

When the technical aspects of these systems are explained to users, how do their choices of settings change?

Nearly 40% of participants modified their settings after being shown an explanation of DNS and encrypted DNS



Recommendations

Provide a basic primer on DNS function (and privacy risks)

- Explain DNS function, privacy risks, tradeoffs associated with each setting

Provide privacy policies for the resolvers

- Will lead to more informed choices
- Will help users understand the differences between the recursive resolvers

Be thoughtful of the technical protocol terminology

- DNS-over-HTTPS name confusion

Provide users with the necessary format to select a custom resolver

- Add instructions, guidelines, and warnings for more clarity

Recommendations

Provide a basic primer on DNS function (and privacy risks)

- Explain DNS function, privacy risks, tradeoffs associated with each setting

Provide privacy policies for the resolvers

- Will lead to more informed choices
- Will help users understand the differences between the recursive resolvers

Be thoughtful of the technical protocol terminology

- DNS-over-HTTPS name confusion

Provide users with the necessary format to select a custom resolver

- Add instructions, guidelines, and warnings for more clarity

Recommendations

Provide a basic primer on DNS function (and privacy risks)

- Explain DNS function, privacy risks, tradeoffs associated with each setting

Provide privacy policies for the resolvers

- Will lead to more informed choices
- Will help users understand the differences between the recursive resolvers

Be thoughtful of the technical protocol terminology

- DNS-over-HTTPS name confusion

Provide users with the necessary format to select a custom resolver

- Add instructions, guidelines, and warnings for more clarity

Recommendations

Provide a basic primer on DNS function (and privacy risks)

- Explain DNS function, privacy risks, tradeoffs associated with each setting

Provide privacy policies for the resolvers

- Will lead to more informed choices
- Will help users understand the differences between the recursive resolvers

Be thoughtful of the technical protocol terminology

- DNS-over-HTTPS name confusion

Provide users with the necessary format to select a custom resolver

- Add instructions, guidelines, and warnings for more clarity

User Awareness and Behaviors Concerning Encrypted DNS Settings in Web Browsers

Alexandra Nisenoff, Ranya Sharma, Nick Feamster

- Work is needed to:
 - Improve user awareness
 - Provide users with more information
 - Design intuitive setting interfaces

Acknowledgements

This work was supported by NSF Award SaTC-2155128, NSF Award TWC-1953513