User Awareness and Behaviors Concerning Encrypted DNS Settings in Web Browsers

Alexandra Nisenoff, Ranya Sharma, Nick Feamster



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





Wew lab x +							×
← → G (G)					<u>(</u>) 🖈) 🔊 🕲 🕲		R
🦧 case number 🔇 scansion 🧕 Home Schoology 背 Data S	itructures T 🙎 About BHS / Bell S	C Campus Studer	it 📑 Google Doo	cs 🔇 🌍 New Tal	ib 🕄 (New Tab		ЖТ
					New Window		ЖN
					New Incognito Wind	ow	Ġ₩Ν
					History		•
					Downloads		Σ₩L
					Bookmarks		•
	C		1.0		Google Password M	anager New	
	(7				Extensions		•
					Zoom	- 100% +	13
					Print		ЖР
					Cast		
	Q Search Google or type a	a URL		🌷 😨 🌖	Find		₩F
					More Tools		•
					Edit	Cut Copy	Paste
				20	Settings		ж,
	The Universit Workday@UC	Google Docs	YouTube	July 2023	Help	\	
	(1) (1)	alt	in	+		√ <u>→</u>	
					V	Ú	
	Canvas LMS Reflexive Ver	Gradescope	(15) Feed	Add shortcut		-	
						Customize Cl	nrome

•	• Settings × +											~
÷ -	C O Chrome chrome://settings		Û	☆	2	0	3 🧐	3	*	=J [R	:
0	Settings	Q Şearch settings										
÷	You and Google	You and Google										
i t	Autofill and passwords Privacy and security	Get Google smarts in Chrome Sync and personalize Chrome across your devices										
Q	Performance	Ranya Sharma ranyasharma@uchicago.edu	1C									
e Q	Appearance Search engine	Sync and Google services	•									
	Default browser	Manage your Google Account	Ø									
ባ	On startup	Customize your Chrome profile	•									
۲	Languages	Import bookmarks and settings	•									
<u>+</u>	Downloads											
Ť	Accessibility											
0	System Reset settings											
*	Extensions											
chrome	About Chrome											
cmome:	Jsettings/privacy											



• •	• Settings - Security × +												~
$\leftarrow \rightarrow$	C O Chrome chrome://settings/security		₫	☆	2	C	e	1 00	M	* =	=J [] (3
0	Settings	Q Search settings											
÷	You and Google	you about password breaches. Requires browsing data to be sent to Google.											
Ê	Autofill and passwords	Standard protection Standard protection against websites, downloads, and extensions that are known to be	~										
0	Privacy and security	dangerous											
	Performance	No protection (not recommended) Does not protect you against dangerous websites, downloads, and extensions. You'll still get Safi 	e										
۲	Appearance	Browsing protection, where available, in other Google services, like Gmail and Search.											
Q	Search engine	Advanced											
	Default browser												
Ċ	On startup	Upgrade navigations to HTTPS and warn you before loading sites that don't support it											
	Languages	Use secure DNS Determines how to connect to websites over a secure connection											
<u>+</u>	Downloads	With your current service provider		N									
Ť	Accessibility	Secure DNS may not be available all the time			\backslash								
٩	System	With Custom -			١٢	7							
9	Reset settings		ļ		ν								
*	Extensions 🔀	Manage security keys Reset security keys and create PINs	÷										
(9)	About Chrome	Manage device certificates Manage HTTPS/SSL certificates on your device	Z										

← -}	C O Chrome chrome://settings/securit		Û	☆	5	G	e	100	*	≡J	R	:
0	Settings	Q Search settings										
÷	You and Google	you about password breaches. Requires browsing data to be sent to Google.										
Ê	Autofill and passwords	Standard protection O Standard protection against websites, downloads, and extensions that are known to be	~	,								
•	Privacy and security	dangerous										
Ø	Performance	No protection (not recommended) Oes not protect you against dangerous websites, downloads, and extensions. You'll still get Sa	afe									
۲	Appearance	Browsing protection, where available, in other Google services, like Gmail and Search.										
Q	Search engine	Advanced										
	Default browser	Auvanceu										
ባ	On startup	Always use secure connections Upgrade navigations to HTTPS and warn you before loading sites that don't support it	0									
•	Languages	Use secure DNS Determines how to connect to websites over a secure connection										
<u>+</u>	Downloads											
Ť	Accessibility	Secure DNS may not be available all the time										
3	System	● With Custom ▼										
•	Popot pottingo	google.com										
.9	noor orningo	Enter a correctly formatted URL										
*	Extensions	Manage Reset se vanue create PINs	÷									
9	About Chrome	Manage device offificates	Ľ	3								

ightarrow C () Chrome chrome://settings/secu	ty	Û	☆	2	C	e	1	*	≡J	R	;
Settings	Q Search settings										
You and Google Autofill and passwords Privacy and security Performance	you about password breaches. Requires browsing data to be sent to Google. Standard protection Standard protection against websites, downloads, and extensions that are known to be dangerous No protection (not recommended)	~									
Appearance Search engine Default browser	 Does not protect you against dangerous websites, downloads, and extensions. You'll still get Safe Browsing protection, where available, in other Google services, like Gmail and Search. Advanced Always use secure connections 										
Constantup Languages Languages Downloads Accessibility System Reset settings	Upgrade navigations to HTTPS and warn you before loading sites that don't support it 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 Custom https://dns.google/dns-query										
Extensions	Manage security keys Reset security keys and create PINs	÷									
About Chrome	Manage device certificates Manage HTTPS/SSL certificates on your device	Z									

Enabling DNS-over-HTTPS



Choosing a Trusted Resolver

✓ Custom

CleanBrowsing (Family Filter) Cloudflare (1.1.1.1) NextDNS OpenDNS Google (Public DNS)

Enter custom provider

OpenDNS

Quad9 (9.9.9.9)

CleanBrowsing (Family Filter)

NextDNS

Google (Public DNS)

Cloudflare (1.1.1.1)



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



Our Study Methods

Screening Survey

Browser usage

800 participants

Our Study Methods

Screening Survey

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



Preliminary understanding of DNS









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**.



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**.



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.

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/d ns-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 <u>Secure DNS</u> 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 <u>DNS-over-HTTPS</u> 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



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

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

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

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