User Awareness and Behaviors Concerning Encrypted DNS Settings in Web Browsers

Alexandra Nisenoff, Ranya Sharma, Nick Feamster
Motivation

- Current encrypted DNS ecosystem has a power imbalance
  - Interferes with technical design

- Design choices affect
  - Market consolidation
  - User privacy
  - User experience
DNS

User’s device

Recursive Resolver

Web Server

ucheicago.edu

3.215.148.80

website content
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
Determine how to connect to websites over a secure connection

- With your current service provider
  Secure DNS may not be available all the time
- With OpenDNS
  See this provider’s privacy policy

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
  Enter custom 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.

- Cloudflare (default)
- Cloudflare for Families (No Malware)
- Cloudflare for Families (No Malware or Adult Content)
- Google Public DNS
- Enter Custom DNS server address

Do not prompt for authentication if password is saved
Proxy DNS when using SOCKS v5
Enable DNS over HTTPS

Use Provider Cloudflare (Default)

Help Cancel OK
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

Preliminary understanding of DNS

Interactive versions of browsers

Explanation of DNS given

n = 45  n = 48  n = 40  n = 51
Main Survey

- Preliminary understanding of DNS (n = 45)
- Interactive versions of browsers (n = 48)
- Explanation of DNS given (n = 40)
- Interactive versions of browsers (n = 51)
Main Survey

Preliminary understanding of DNS

Interactive versions of browsers

Explanation of DNS given

Interactive versions of browsers

Check settings in own browser

n = 45
n = 48
n = 40
n = 47
n = 34
n = 4
n = 51
n = 26
n = 71
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**.

- **73%** heard of DNS
- **27%** did not hear of DNS
- **59.9%** heard of encrypted DNS
- **40.1%** did not hear 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

- 79.4% selected default
- 20.6% did not select default

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

“McAfee”

“www.google.com”

“1.1.1.1”

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.

- Modified settings: 37%
- Did not modify settings: 63%
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