Symposium On Usable Privacy and Security 2026

I See DNS People

DNS Resolver Security, Through Operator Perspectives and Practices

Wisdom Obinna, Katharina Barlage, Florian Alt, Harel Berger

GEORGETOWN UNIVERSITY

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

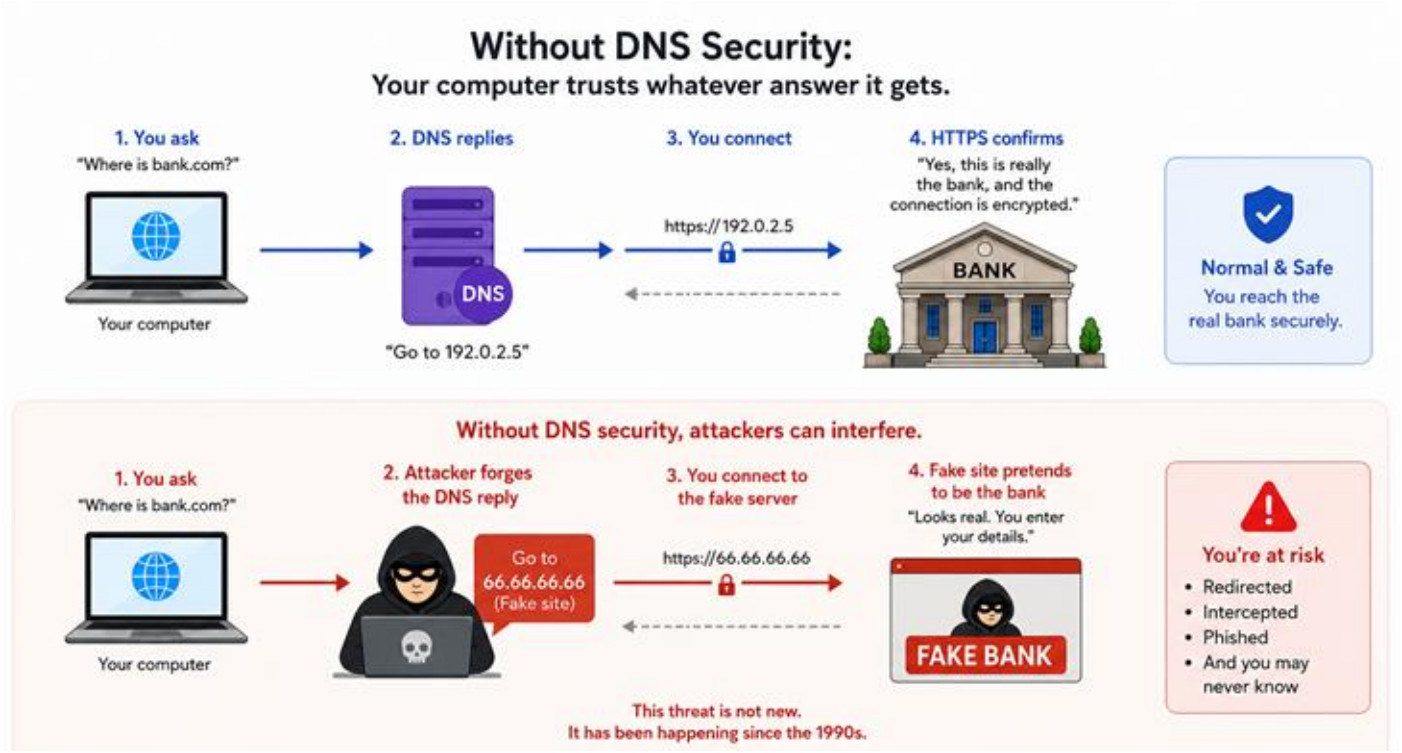
ARIEL UNIVERSITY






Why Should I Care?

Why should I care?



Why should I care?

A denial-of-service attack on one DNS provider disrupted Twitter, Netflix, and dozens of major services for hours

A race condition in an internal DNS management system triggered a 14-hour outage across multiple countries.

https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service







https://www.thousandeyes.com/blog/aws-outage-analysis-october-20-2025(2025)

DNSSEC has been standardized for **30 years**.
Adoption is low and slow

We know *what* operators deploy.
Not *why* they choose it or do not.

5.5% of domains sign with DNSSEC

12% of resolvers validate responses

Organizational constraints & priorities

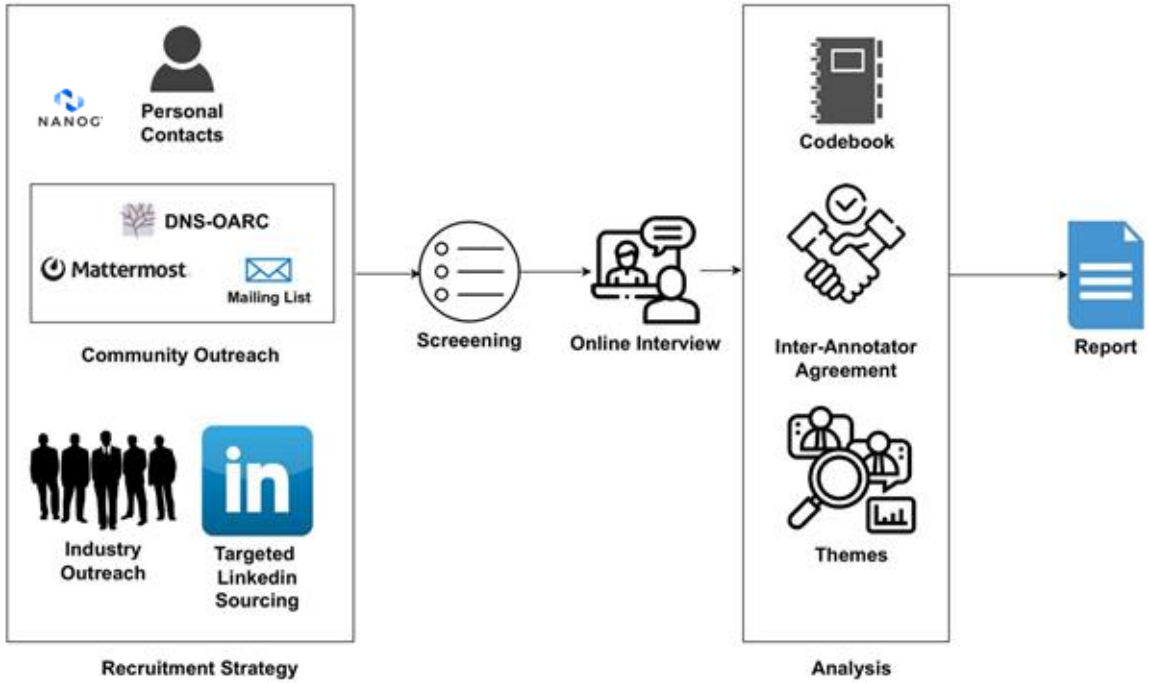
Perceived risks of change

Human decision-making processes

Research Questions

1. **What shapes prioritization?**
   What factors shape how DNS operators prioritize security relative to other operational concerns?
2. **How are mechanisms perceived?**
   How do operators perceive and experience specific DNS security mechanisms?
3. **What enables adoption?**
   What conditions enable DNS security adoption? What interventions do operators deem most effective?

Research Process



Participants

24

resolver operators
& practitioners

23

organizations across
ISPs, enterprise, gov



14

countries in Europe,
Asia, Africa, Americas

45–60

minutes per
remote interview

Who they are

14 **Enterprises**

the dominant organizational context

6 **Service providers**

ISPs, DNS vendors, managed services

4 **Consultants**

including one government role

9 **Security engineers & architects**

largest single role cluster

DNS “just works” (so nobody cares until…)

A self-reinforcing cycle

Availability outranks security

Security is assumed, not assessed

18/24

described environments where DNS security is deprioritized until failure

“They never understand the criticality until it goes down.”

— P20

The risk feels one-sided

If you do nothing, everything may look fine

If you set it up incorrectly, everyone notices

The incentive is backwards

13/24

said they'd never had a real DNS incident — so the danger stays abstract

"If you touch something that's working, you might break it…"

— P17

DNSSEC: intimidating before, manageable after

Before Deployment

“Intimidating”



After Deployment

“Really easy to set up”

8 of 13 deployers — 6 of them initially intimidated

DNSSEC: intimidating before, manageable after

When we probed further…

1 **Dense documentation design**

Conflates conceptual theory with operational setup.

DNSSEC: intimidating before, manageable after

When we probed further…

1 **Dense documentation design**

Conflates conceptual theory with operational setup.

2 **Cryptographic Jargons**

Terminology sounds harder than the operations warrant.

DNSSEC: intimidating before, manageable after

When we probed further…

1 Dense documentation design

Conflates conceptual theory with operational setup.

2 Cryptographic Jargons

Terminology sounds harder than the operations warrant.

3 Peer narratives of failure

Community stories emphasize failure over routine success.

Thin expertise, delegated trust

16/24

cited a lack of expertise
(the single most common barrier)

8/24

delegated DNS protection to vendors
(trust over verification)

2-Person Teams

micro-teams of up to 2 people managing global DNS were a common pattern.

> *I am shocked constantly with how little is known about DNS by the security industry. The expertise is extremely thin in truly understanding DNS security.*
>
> — P2

A lesson from TLS

TLS / HTTPS

- ✓ Browser enforcement — warnings punish non-HTTPS sites
- ✓ Zero-cost automation via Let's Encrypt & ACME
- ✓ A single operator can deploy it unilaterally

DNSSEC

- — No comparable enforcement pressure to compel adoption
- — Chain of trust needs operator, registrar & parent zone
- — No single party can complete deployment alone

What each audience can do



Tool developers & standards bodies



DNS operators



Policymakers

In summary: DNS Resolver Security, Through Operator Perspectives and Practices

Organizational behavior outweighs technical factors

01 DNS security is systematically deprioritized — noticed only when it fails.

02 Getting started with DNSSEC seems more complicated than it actually is.

03 Better protocols alone cannot solve gaps in expertise and resources.

Recommendation: Make DNSSEC easier to understand,
make its security benefits visible, and require adoption where voluntary efforts stall.



The paper



Contact
Wisdom Obinna