Your Internet Might Not Be As Private As You Think

What We Found When We Put the Internet's DNS System to the Test

By © CoreNetSolution Published: July 2025 Contact: Website: corenetsolution.com

What Is This About?

Every time you visit a website, your device asks a background service called **DNS** (Domain Name System) to find the right destination. It's like your internet's phonebook — it connects you to websites.

But here's the catch: even when everything is locked down — encrypted, secured, and seemingly private — your system might still be quietly sending requests to **servers you didn't approve or even know about**.

This report reveals how **we tested extremely secure setups**, only to discover that **our data still leaked to outside networks — silently, invisibly, and globally**.

What We Discovered

In our controlled testing of well-secured systems, we found:

- Up to **65 different DNS servers**, located all over the world, were responding to our internet requests
- Some were located in regions like **Europe, Asia, and North America**, far outside the networks we configured
- These unauthorized responses occurred on both **home broadband and mobile connections**, even inside encrypted environments

Even more concerning: everything looked "normal" from the user's point of view. There were no errors, no alerts — just background leakage most people would never notice.

Why It Matters

Your DNS activity silently reveals:

- What websites you visit
- When you access them
- How often you return

This can happen **even when your actual browsing is encrypted.** If the DNS path leaks, your privacy leaks too — especially if:

- Your internet provider silently rewrites your DNS traffic
- Your device "falls back" to other servers without asking
- Other networks reroute your request for "optimization" without your consent

A Real-World Example: Login Breaks When DNS Breaks

During testing, we tried logging into a trusted online control panel. But it failed — looping with this message:

> **“auth.ionos.com redirected you too many times.”**

No cookies, DNS flushes, or browser resets solved it.

Our theory? The system’s login logic broke down because DNS requests were **rerouted through unauthorized paths**, causing the session to misfire.

It may seem like a tech glitch, but these small cracks reflect the bigger issue: if DNS can shift invisibly, so can the security protections built on top of it.

How We Tested It

We designed our experiment to **lock down everything**:

- Used encrypted DNS only (like DNS-over-TLS)
- Disabled browser-based DNS overrides
- Monitored DNS traffic using packet capture tools (like `tcpdump`)
- Verified no proxies, VPNs, or split tunnels were in use
- Ran leak analysis using independent tools like VPNTesting and BrowserScan

Even under those strict conditions, **our DNS traffic was intercepted and handled by third parties** — sometimes halfway across the world.

Where Did Our Queries Go?

Leak tests revealed responses from:

- Data centers and ISP endpoints in multiple countries
- Cloud CDN edge servers we never opted into
- Recurring networks with no documented connection to our systems

We never configured them. But they still got our requests.

What You Can Do About It

Here’s how regular internet users — even non-techies — can fight back:

- **Run a DNS leak test** once in a while. Try tools like or
- **Check your browser or device settings** and disable automatic DNS overrides where possible
- **Ask questions** — your internet provider, browser, and apps should tell you clearly how they handle DNS. You deserve to know who’s routing your data.
- **Talk about it publicly** — the more people notice and question, the harder it becomes for silent rerouting to hide in the shadows

> **Important**: Changing your DNS server might help in certain cases — but this goes deeper. It’s about making sure **every DNS provider and network actually respects your settings** and doesn’t reroute traffic in the background.

Our Final Thoughts

We set out to confirm secure DNS behavior — and instead uncovered a quiet, systemic problem. Despite locking down every setting available, DNS still leaked through networks we never selected.

This isn’t just about privacy. It’s about **trust** — in your tools, your providers, and the rules of the road online.

So here’s what we believe:

- **Every user deserves transparency** — know where your data goes
- **Every network should be accountable** — stop silently rewriting DNS
- **Every device should obey your choices** — and stop falling back to unknown systems

The internet doesn’t have to be a black box. Let’s bring DNS resolution into the light — together.

Additional Note: Time of Day and Resolver Behavior

During late-night testing, DNS leak tests unexpectedly returned clean — even on systems where daytime sessions had shown high leakage rates.

Why? One possible explanation is that during off-peak hours, internet traffic is lighter, and local DNS servers may be able to fully respond from cache. This reduces their need to forward requests to external servers — a behavior more common during daytime or high-load conditions.

This suggests:

- **DNS leakage may not be a constant**, but a function of system load, traffic, and time of day
- A network that appears secure at night may leak during peak hours
- Resolver transparency is a **moving target**, not a static condition

Bottom line: Even without changing your configuration, DNS trust boundaries may shift behind the scenes — silently, dynamically, and without notice.

DNS Forwarding Should Respect Trust Boundaries

Let’s be clear: **DNS forwarding itself isn’t the issue**. It’s a powerful and valid design tool — especially when used under your own control, like forwarding from a secondary server to a primary inside a trusted environment.

But when **internet providers forward your DNS queries to third-party services without disclosure**, they cross a line:

- They undermine user consent
- They expose private lookups to outside networks

- They bypass transparency and accountability

Operators at scale should maintain **resilient, self-contained DNS resolution infrastructure** — backed by regional data center caches, encrypted transport, and full recursion capabilities — without defaulting to third-party relay points.

> Forwarding should never mean “offloading privacy.” It should mean routing — with control, encryption, and purpose.

Resolvers must:

- Maintain encrypted resolution paths end to end
- Document and disclose recursive behavior
- Avoid rewriting, rerouting, or failing silently

This isn’t about condemning tools. It’s about safeguarding trust — the foundation on which DNS, and the internet itself, depend.