MY WEIRD PROMPTS

Podcast Transcript

EPISODE #220

Beyond HTTPS: Securing Your Digital Shadow with Private DNS

Published January 13, 2026 • Runtime: 13:36

https://myweirdprompts.com/episode/encrypted-dns-privacy-guide/

EPISODE SYNOPSIS

Even when you use encrypted websites, your Internet Service Provider can still see every domain you visit through unencrypted DNS queries. In this episode of My Weird Prompts, Herman and Corn dive into the world of Private DNS, explaining how protocols like DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH) can shield your browsing metadata from prying eyes. They break down the benefits of popular providers like Cloudflare, Quad9, and Mullvad, while addressing the limitations of using encrypted DNS without a VPN. Whether you're an Android user looking to flip a switch or an iOS user managing profiles, this episode provides a clear, technical roadmap to reclaiming your digital privacy and building "privacy herd immunity."

DANIEL'S PROMPT

Daniel

I’m interested in DNS over HTTPS and encrypted DNS. If I choose to use a custom DNS server on my Android phone instead of the default, what are the privacy benefits of doing this in isolation, and what are the main DNS options available?

TRANSCRIPT

Corn

You ever get that feeling that you are being followed, but not by a person? It is more like a digital shadow that knows every single website you visit, even if you are using an encrypted connection like H-T-T-P-S?

Herman

Herman Poppleberry here, and I know exactly what you are talking about, Corn. It is the great irony of the modern web. We have all these layers of security, yet the very first step we take to find a website is often wide open for anyone on the network to see.

Corn

It is like locking your front door but leaving a map on the porch showing exactly where you went for dinner. And that is exactly what our housemate Daniel was asking about in his prompt this week. He noticed that setting in the Android menu for Private D-N-S and wanted to know if switching to a custom, encrypted D-N-S server actually does anything for your privacy if you are not doing anything else, like using a Virtual Private Network.

Herman

It is such a great question because it gets to the heart of how the internet actually functions under the hood. Most people think H-T-T-P-S protects everything, but it really does not.

Corn

Right, and I think we should really dig into the mechanics here. We have touched on security before, like back in episode two hundred and sixteen when we talked about C-V-Es and CrowdSec, but this is different. This is about the fundamental plumbing of the internet. So, Herman, for those who might have a general idea but want the technical nuance, what exactly is the problem with standard Domain Name System requests?

Herman

Well, the Domain Name System, or D-N-S, is essentially the phonebook of the internet. When you type in a website name, your computer has to ask a D-N-S server for the numerical Internet Protocol address, or I-P address, associated with that name. The problem is that, historically, these requests are sent in plain text. They are unencrypted.

Corn

And that means anyone sitting between you and that D-N-S server can see exactly what you are looking for.

Herman

Exactly. That includes your Internet Service Provider, the person running the Wi-Fi at the coffee shop, or even a malicious actor on the same network. Even if the website you eventually visit uses H-T-T-P-S to encrypt the actual content of your visit, the initial request to find that website is broadcast to the world.

Corn

So, even if my I-S-P cannot see the specific page I am reading on a site or the data I am sending, they know I am visiting that site. They see the metadata.

Herman

Precisely. And in twenty-twenty-six, metadata is big business. Internet Service Providers can and do log these requests. They build a profile of your interests, your health concerns, your political leanings, all based on the domains you resolve. With modern A-I-driven traffic analysis, they can even predict your future behavior based on those patterns. They then sell that anonymized data to advertisers.

Corn

That is the part that always gets me. I am paying them for a service, and they are essentially double-dipping by selling my browsing habits. But Daniel specifically asked about the benefits of changing this in isolation. If I go into my Android settings right now and switch to an encrypted D-N-S provider, what actually changes for me?

Herman

This is where it gets interesting. On Android, when you use the Private D-N-S feature, it uses a protocol called D-N-S over T-L-S, or D-o-T, with D-N-S over H-T-T-P-S, or D-o-H, available in browsers like Chrome on Android 15 and 16. Both do essentially the same thing: they wrap those plain text D-N-S queries in an encrypted tunnel.

Corn

Okay, so the I-S-P sees that I am talking to, say, Cloudflare or Google, but they cannot see the names of the websites I am asking for within that tunnel.

Herman

That is the primary benefit. It effectively blinds your I-S-P to your D-N-S history. It also prevents D-N-S hijacking. That is a technique where a network operator redirects your request for a legitimate site to a malicious one. If the D-N-S request is encrypted and authenticated, they cannot mess with the answer you get back.

Corn

But here is the catch I was thinking about. Even if the D-N-S request is encrypted, do I not still have to connect to the I-P address of the website? And does my I-S-P not see that I-P address?

Herman

You have hit on the exact limitation of doing this in isolation. Yes, the I-S-P still sees the destination I-P address. However, a huge portion of the modern web sits behind content delivery networks like Cloudflare or Akamai. Hundreds of thousands of websites might share the same I-P address. In those cases, the I-S-P knows you are talking to a Cloudflare server, but they do not know which specific website on that server you are visiting. It creates a level of ambiguity that makes mass profiling much harder.

Corn

Ah, so it is not perfect, but it is a significant step up from broadcasting every domain name in plain text. But what about that other leak you mentioned? The S-N-I?

Herman

Right, Server Name Indication. Historically, even with encrypted D-N-S, the domain name leaked during the H-T-T-P-S handshake. But here is the good news for twenty-twenty-six: a newer standard called Encrypted Client Hello, or E-C-H, is increasingly supported. It encrypts that initial handshake too. Browsers like Firefox and providers like Cloudflare support it, helping to close that metadata leak when enabled.

Corn

That sounds like a massive win for privacy. But let us talk about the options. Daniel wanted to know what is out there. If someone wants to make this switch on their phone, who are the big players?

Herman

There are several excellent options. The most well-known is Cloudflare's one-dot-one-dot-one-dot-one. They are incredibly fast and have a strong privacy policy, claiming to delete logs within twenty-four hours. Then there is Quad-Nine, the nine-dot-nine-dot-nine-dot-nine service. They are a non-profit based in Switzerland, and they actually block known malicious domains at the D-N-S level, which is a great security bonus.

Corn

I like the idea of a non-profit. What about the more customizable ones?

Herman

Next-D-N-S is the gold standard for control freaks. It is like having a Pi-hole in the cloud. You can toggle on blocklists for Facebook trackers, ad networks, or even entire categories of sites. It saves battery and data because your phone never even attempts to download those ad assets. There is also AdGuard D-N-S, which is very user-friendly for ad-blocking.

Corn

And I have heard people mentioning Mullvad D-N-S lately too.

Herman

Oh, absolutely. Mullvad is a favorite in the privacy community. They have a public D-N-S that is completely free, supports Do-H and Do-T, and they have a legendary reputation for not keeping any logs whatsoever. It is a great choice if you want to stay away from the big tech ecosystems entirely.

Corn

So, we have Cloudflare for speed, Quad-Nine for security, Next-D-N-S for customization, and Mullvad for pure privacy. What about Google? They are the default for a lot of people.

Herman

Google's eight-dot-eight-dot-eight-dot-eight is reliable, but if your goal is privacy from big tech, using Google as your D-N-S provider is a bit like asking the fox to guard the henhouse. They already know so much; giving them your D-N-S queries just completes the puzzle for them.

Corn

Fair point. So, for Daniel and everyone else, the takeaway is: yes, changing your D-N-S in isolation is absolutely worth it. It is not a total invisibility cloak—you still need a V-P-N or Tor for that—but it is like putting up curtains in your house. People can still see that the lights are on, but they cannot see what you are doing inside.

Herman

Exactly. It is about raising the cost of surveillance. And it is so easy to do. On Android, it is usually under Settings, then Network and Internet, then Private D-N-S. You just select Private D-N-S provider hostname and type in the address. For Cloudflare, it is one-dot-one-dot-one-dot-one-dot-cloudflare-dot-dns-dot-com. For Quad-Nine, it is dns-dot-quad-nine-dot-net.

Corn

And for our i-O-S listeners, it is a bit different, right?

Herman

Right. On i-O-S, you usually install a configuration profile. Most of these providers have simple apps that will generate that profile for you in seconds. Once it is on, it works system-wide just like on Android.

Corn

One minor downside we should mention is the captive portal issue. You know, those login pages at airports or hotels?

Herman

Yes, they often break because they rely on intercepting your D-N-S to show you that login page. If your phone is locked to an encrypted provider, it might just show a connection error. The fix is simple: temporarily turn off Private D-N-S, log in to the Wi-Fi, and then toggle it back on.

Corn

That is a small price to pay for twenty-four-seven privacy. And Herman, you mentioned that some browsers have their own settings too?

Herman

Yes, Chrome and Firefox often have a 'Secure D-N-S' toggle. Usually, the Android system-wide setting takes precedence, but it is always worth checking your browser settings to make sure you are not accidentally bypassing your custom provider. It is about making sure all the windows are closed, not just the front door.

Corn

I love that. It is like privacy herd immunity. Every person who switches makes the whole network a little more secure and a little less profitable for snoops.

Herman

I love that framing! Privacy herd immunity. We should trademark that.

Corn

Ha! Good luck. Well, I think we have covered every nook and cranny of this topic. Daniel, I hope that helps you navigate your Android settings.

Herman

And for everyone else, stay curious and keep those prompts coming. No topic is too obscure for us.

Corn

We really do live for this stuff. If you want to find our back catalog or subscribe to our R-S-S feed, head over to my-weird-prompts-dot-com. And if you have a second, leave us a review on Spotify—it really helps other curious minds find the show.

Herman

Herman Poppleberry, signing off.

Corn

And Corn too. Thanks for listening to My Weird Prompts. Now, let's go find that coffee.

Herman

Lead the way, Corn. Just don't block the coffee shop's Wi-Fi with your new filters.

Corn

No promises! Goodbye, everyone!

Herman

Bye!