Here’s How To Plug One Of The Biggest Privacy Holes In The Internet

An upgrade to DNS, the internet’s address book, would make it harder for ISPs to know where you surf, and for hackers to hijack your traffic.

[Photo: Flickr user Yuri Samoilov]

BY SEAN CAPTAIN 5 MINUTE READ

Last March, Congress gave internet service providers the green light to collect user data—without their consent—when it abolished an FCC regulation aimed at strengthening internet privacy. While a few states are struggling to enact their own ISP privacy laws, private companies, academics, and nonprofits are coming up with technical workarounds that would diminish the ability of ISPs to eavesdrop on their customers.

Two new projects have just launched that seek to do that by upgrading DNS, the internet's address book, so ISPs can't easily see what web page you're navigating to. The projects will also make everyone safer from hackers who want to hijack your web traffic. Today, Mozilla and Cloudflare fired up a privacy remedy using a new encrypted version of DNS. Meanwhile, researchers at Princeton have proposed another DNS tweak to further obfuscate your surfing.

PATCHING THE INTERNET'S LEAKY PLUMBING

DNS, the domain name system, translates easy-to-remember addresses of websites, like google.com, to the numerical representations (IP addresses) that the internet uses, such as 172.217.7.196. You're automatically connected to an ISP's own DNS server when you log onto a home router or public hotspot, or when your cellphone connects to the network. In the process, the ISP gets a log of everywhere you go online.

But you can plug the IP address of a different DNS server into your computer's or phone's operating system. Google, for instance, operates a free DNS service at IP address 8.8.8.8 that's helped people get online when repressive regimes try to thwart connectivity by sabotaging other DNS servers.

Now Cloudflare is launching a free, privacy-focused DNS at the address 1.1.1.1, and it's partnering with Mozilla to support an encrypted connection with the Firefox web browser. Cloudflare is one of the big content delivery networks that sit between websites

and the open internet, shielding them from cyber attacks and speeding up delivery of their content. But 1.1.1.1 is available to any user or site, not just Cloudflare customers.

SETTING IT UP

You first need to set your device to use Cloudflare's DNS servers. The company provides instruction videos on the service's landing page for the Windows, macOS, Android, and iOS operating systems. Even taking this step will provide a modicum of privacy. In bypassing your ISP's DNS servers, it won't be collecting your page requests automatically.

Changing the DNS server address on an iPhone to 1.1.1.1 and backup server 1.0.0.1. [Animation: courtesy of Cloudflare]

For better security, you need to set up an encrypted connection between Cloudflare and your web browser or app, using a new technology standard called DNS over HTTPS. Like the encrypted connection that protects data you exchange with your bank's website, this new tech encrypts the identity of the site you are

visiting. Firefox is the first major web browser to offer this, not in the standard download version, but in the beta versions offered on its site.

An ISP's routing system does need to know what website to connect your computer to. So it could still sniff out the IP addresses of the pages it delivers to you, look up what sites they belong to, and build a user web-surfing profile. But that requires a lot more work than just reading the logs from its own DNS server.

WHO CAN YOU TRUST?

“What this system is doing is shifting trust from your ISP to another party. You have to decide if you’d rather trust them instead,” says Nick Feamster, a Princeton computer science professor who specializes in networking technology.

Cloudflare has faced criticism over free-speech absolutism that allows nasty customers like the *Daily Stormer*, a neo-Nazi site, to use its service. (Cloudflare finally booted the site last year.) But the company also has a positive image for supporting net neutrality and fighting censorship. Its Project Galileo, for instance, protects sites with humanitarian and politically dissenting content from cyber-attacks by governments or vigilantes.

“[W]e have to have privacy policies that insure that we will not retain or give away or sell information that we receive from this,” says Cloudflare CEO Matthew Prince. To back that up, Cloudflare is hiring a third-party auditor, KPMG, to certify that it doesn’t keep any of the information about people’s web surfing that passes through its servers.

Feamster says he thinks third-party audits could “add a level of credibility.” So does Ernesto Falcon, legislative counsel at the Electronic Frontier Foundation, a group that tends to be very circumspect in assessing tech companies.

The partnership with the Mozilla Foundation, maker of the Firefox browser, adds another level of cred. “We have a contract, an actual legal agreement,” that Firefox users’ data will not be retained by Cloudflare, says Selena Deckelmann, a senior director of engineering at Mozilla.

Download the beta version of Firefox to try out DNS over HTTPS [Image: courtesy of Mozilla]

So what is Cloudflare getting out of the deal? “The craven business reason that we’re doing this is not around [monetizing customer] data,” says Prince. “The benefit for us is that it makes all of our customers a little bit faster for people who are using [our DNS service].” Cloudflare’s DNS service is currently ranked as the world’s fastest, according to analytics site DNSPerf.

“When you’re running a [content delivery network] it’s super helpful to run the DNS as well,” says Feamster. “It totally makes sense why they would benefit and why they would have no need to keep [customer data] and sell it for advertising.”

Nevertheless, Feamster would prefer that no one have even the capability to know what web pages people are requesting. He’s just introduced a proposed fix, called Oblivious DNS, that keeps everyone in the dark. It’s rather hairy to explain, but the upshot is that it uses a further layer of encryption to separate the IP address of the person requesting a web page from the address of the actual page they are requesting. No single party could connect the two bits

of information. Oblivious DNS would be compatible with what Cloudflare and Mozilla are doing, says Feamster, as another layer of security.

Related: **How To Roll Your Own Net Neutrality**

“It’s exciting to see that Cloudflare is the one that is going ahead and building this,” says Erica Portnoy, staff technologist at EFF. “What would be great to see is every DNS [service] starting doing something to protect [users].”

The DNS-over-HTTPS technology is not exclusive to Cloudflare and Mozilla. It’s an evolving technical standard that anyone can adopt, and it would boost security for the entire internet.

The decades-old DNS system wasn’t designed with security in mind. “By default, all your DNS queries are sent over an unencrypted connection,” says Prince, “which means the hotel you’re staying in, the coffee

shop your surfing the web from, your ISP, anyone who's on the line can see every site that you're visiting." That means hackers listening in on the network can intercept DNS requests and modify the results to direct you somewhere you hadn't intended, such as a website hosting malware.

"This is one of the biggest security holes that we've been trying to patch for 20 or 30 years," says EFF's Portnoy, expressing enthusiasm for DNS over HTTPS. "This is finally something that might actually work, which is honestly amazing."

ABOUT THE AUTHOR

Sean Captain is a technology journalist and editor. Follow him on Twitter @seancaptain. More

You Might Also Like:

How To Roll Your Own Net Neutrality