4 major security risks that Cloudflare DNS can resolve

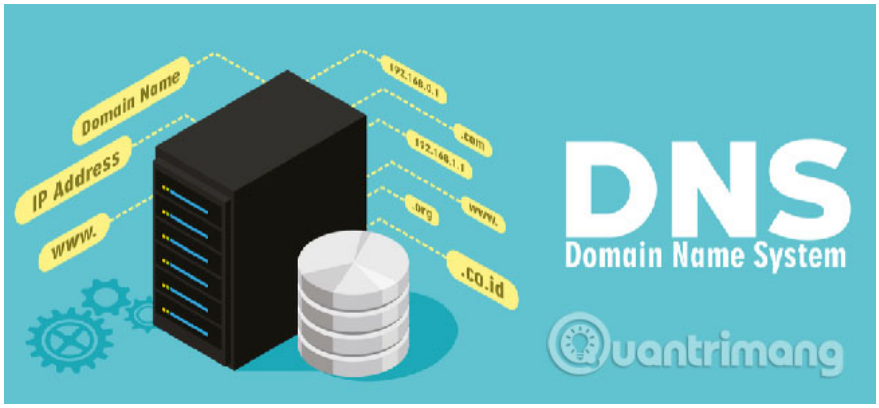
In April 2018, Cloudflare released a new security tool, called 1.1.1.1. This is a consumer DNS address that anyone can use for free.

In April 2018, Cloudflare released a new security tool, called 1.1.1.1. This is a consumer DNS address that anyone can use for free. It can help increase DNS security, improve user privacy and even speed up network connectivity.

But how does it work? How do you use it? And can it help improve DNS privacy risks? Let's take a closer look through the following article!

Learn about Cloudflare DNS - A tool to help resolve DNS-related privacy issues

Problems with DNS and privacy



Domain Name System (DNS) is often called the phone book of the Internet. This is the technology responsible for linking the domains we use every day (for example, quantrimang.com) to the web server's IP address.

Of course, you can enter the site's IP address and still reach its home page, but text-based URLs are much easier to remember, so users often use them.

Unfortunately, DNS technology comes with many privacy-related issues. Problems can affect online safety, even if you take all the usual precautions elsewhere on your system. Here are some of the worst DNS related privacy issues.

1. ISP is watching you

Due to the way DNS works, it acts as a log of the websites you visit. It doesn't matter whether the website you visit uses HTTPS, ISPs, mobile providers and public WiFi providers will still know exactly the domains you have visited.

Worryingly, since mid-2017, US ISPs are allowed to sell customer browsing data to make a profit. In fact, this phenomenon is popular all over the world.

Finally, your browsing history is helping big corporations make money. That's why you must always use a third-party DNS provider.

2. Snooping and spoofing

You are also at risk, because DNS lacks the last mile encryption feature (DNS encryption between devices and ISPs). The cause is:

There are two sides affecting DNS: Competence (toward the content) and recursive resolver - the recursive resolver (towards ISP). In a broad sense, you can think of DNS resolvers by asking questions (for example, where can I find this site?) And DNS nameservers that will provide the answer.

Data moving between the resolver and the authoritative server (theoretically) is protected by DNSSEC. However, the section between the machines (called stub resolver and recursive resolver is not secure).

Sadly, this section creates many opportunities for bad guys to snoop and fake data.

3. The Man-in-the-Middle attack

When you browse the web, the computer will often use cached DNS data somewhere on the network. Doing so may help reduce page load time.

However, this cache itself can become a victim of cache poisoning. This is a Man-in-the-middle attack.

Simply put, hackers can take advantage of poor vulnerabilities and configurations to add fake data to the cache. Then, the next time you visit the site that is 'poisoned', you will be sent to a hacker controlled server.

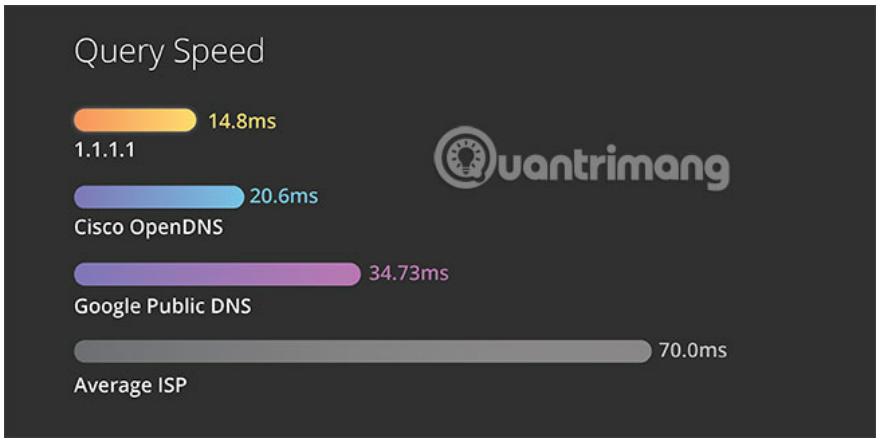
Hackers can even copy your target site. You may never know you were redirected and accidentally entered your username, password and other sensitive information.

This process facilitates a phishing attack.

How does Cloudflare work?

The new 1.1.1.1 service from Cloudflare can overcome many privacy issues related to DNS technology.

The company spent a long time discussing with browser developers and tool developers according to their recommendations, before the service was public.



1. Is Cloudflare DNS safe?

Yes, Cloudflare DNS has no tracking and data storage. Cloudflare has committed to never tracking DNS users or selling ads based on users' habit of viewing everything on the Internet. To reinforce consumer confidence in its claims, the company has stated that it will never save IP address queries to the drive and promises to delete all DNS records within 24 hours.

In fact, that means your DNS history won't fall into the hands of ISPs or any other party.

2. Advanced technology

When you enter the URL and press `Enter` , almost all DNS resolvers send the entire domain name (**www** , **quantrimang** and **com**) to root servers, .com servers and all intermediate services.

All that information is unnecessary. Root servers only need to direct the resolver to .com. The deeper lookup query can be started at that time.

To combat this problem, Cloudflare has added a series of agreed, proposed and recommended DNS privacy mechanisms to connect resolver stub and recursive resolver. As a result, 1.1.1.1 will only send a certain amount of information.

3. Anti Snooping

If you wonder if Cloudflare DNS is secure, the answer is that it is extremely safe. Service 1.1.1.1 provides a feature that helps to prevent Snooping (data snooping): DNS over TLS.

DNS over TLS works by allowing the stub resolver to establish a TCP connection with Cloudflare on port 853. Stub resolver then initializes a TCP handshake and Cloudflare to provide its TLS certificate.

As soon as the connection is established, all communication between the resolver resolver and recursive resolver will be encrypted. As a result, eavesdropping and forgery become impossible.

4. Fight with Man-in-the-Middle attacks

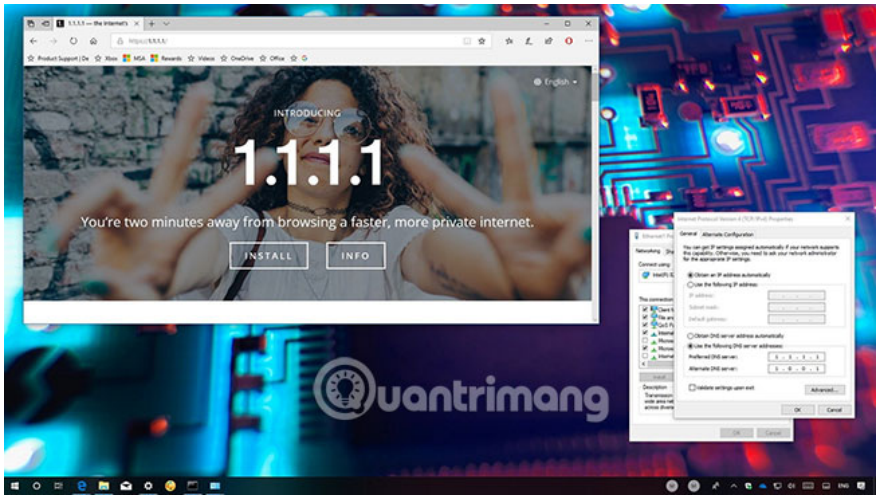
According to Cloudflare, less than 10% of domains use DNSSEC to secure the connection between recursive resolver and authorized server.

DNS over HTTPS is an emerging technology that helps secure HTTPS domains without using DNSSEC.

Without encryption, hackers can 'listen' to your packets and know which web page you are visiting. The lack of encryption also makes it easy to encounter Man-in-the-middle attacks like what the article has detailed before.

How to use Cloudflare DNS

Using the new 1.1.1.1 service is easy. Here, the article explains the process for both Windows and Mac machines.



How to use Cloudflare DNS on Windows

To change the DNS provider on Windows, follow the steps below:

1. Open the **Settings** application from the **Start** menu **.**

2. Go to **Network & Internet> Status> Change your network settings> Change adapter options** .

3. Right-click your connection and select **Properties.**

4. Scroll down, highlight **Internet Protocol Version 4 (TCP / IPv4)** , then click **Properties.**

5. Click **Use the following DNS server addresses** .

6. Enter **1.1.1.1** in the first row and **1.0.0.1** in the second row.

7. Click **OK.**

You may need to restart the computer.

How to use Cloudflare DNS on a Mac

If you have a Mac, follow these instructions to change DNS:

1. Go to **Apple> System Preferences> Network** .

2. Click on the connection in the control panel on the left side of the window.

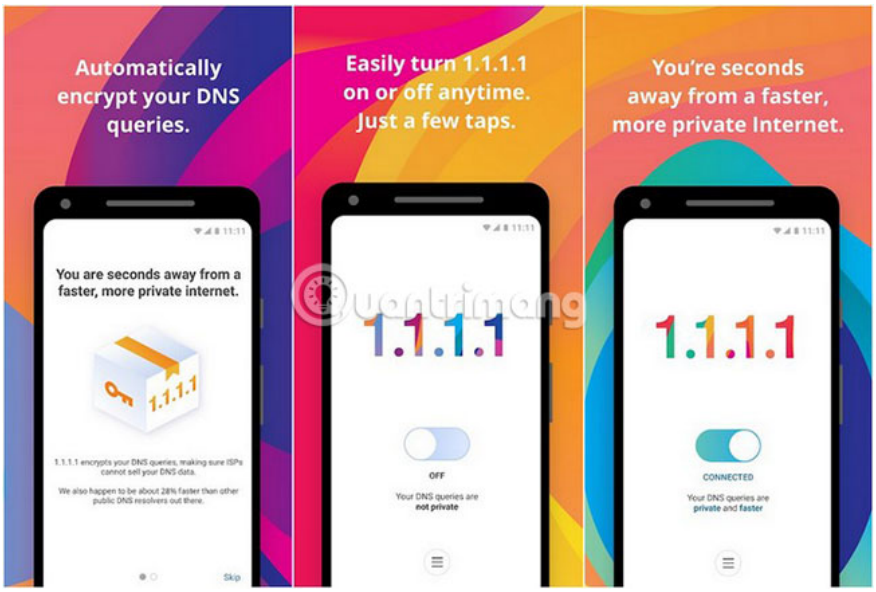
3. Click **Advanced.**

4. Highlight DNS and click the + sign.

5. Enter **1.1.1.1** and **1.0.0.1** into the provided space.

6. Click **OK.**

How to use Cloudflare DNS on smartphones



To use Cloudflare on Android and iOS, you can download the free app from the respective app stores. This Cloudflare DNS application is a recent project from Cloudflare. It was only released in November 2018.

Called 1.1.1.1, the app provides easy-to-use on / off capability for corporate DNS servers. Of course, you can turn on DNS using the phone's original tools, but the installation is not easy to find and some manufacturers even block access to them. This application is much more user-friendly.

Download 1.1.1.1 for Android | iOS (Free).

You must always use strong VPNs in the battle for online privacy. This is more important than having a good DNS.

All reputable VPN providers will also provide their own DNS addresses. However, sometimes you will need to manually update your DNS using the methods that the article detailed above. Failure to do so will result in DNS leaks.

But just because your VPN provider provides their own DNS address, you can still use the Cloudflare address instead. In fact, the DNS of the VPN you are using may be as sophisticated or powerful as the new 1.1.1.1 service.

If you are looking for a solid and reputable VPN provider, you should use ExpressVPN, CyberGhost or Private Internet Access.

And if you want to find out more, make sure you look at **TipsMake.com** 's instructions about what DNS servers are and how DNS cache poisoning works.

Hope you are succesful.