DNS Explained

[video narration]

Is your DNS vulnerable? This video will explain how exposed DNS requests put your privacy at risk. But first, what is DNS?

When you think of the name of a website, you probably think of a URL, like google.com.
But to computers, the true name of a website is an IP address, like 74.125.22... well, you get the idea.

You probably can't keep track of all these numbers, but your computer can. At least for websites you've visited before.

For every new website, your computer needs to ask for the right IP address through a complicated system called DNS, or Domain Name System.

When you type in a new URL, your computer asks a DNS server to find a certain IP address.

The request is sent through a distributed hierarchy of servers, each of which may or may not be able to fill the request, often simply pointing the request in the right direction until the correct IP address is found and delivered back to your computer, all in less time than it takes you to blink.

Most Internet users are configured by default to use unencrypted DNS.

Unfortunately, governments and other organizations sometimes don't want you to see certain content, and intercepting your DNS requests is one of the easiest ways to deny you access.

Unencrypted DNS is also vulnerable to hacks that redirect you to websites designed to scam you

DNS servers also tend to log information, like which websites you visit, when, and from where.

Some VPN providers don't handle their own DNS, so even if your normal Internet traffic is protected, your DNS requests will still be vulnerable.

ExpressVPN runs its own DNS on every server.

Because it never leaves the VPN tunnel, ExpressVPN's DNS is fast, leaves no identifiable information, and, best of all, *all* your DNS queries are signed and encrypted, so they're protected from anyone seeing them, stopping them, or modifying them.

So get the VPN with its own DNS. Get ExpressVPN.