

Over the past few weeks I have been seeing reports that some ISP's are actually subverting DNS queries to their own DNS server. Oh the humanity! What this means is that when you (your computer) does a UDP or TCP Port 53 DNS query the ISP is intercepting that and directing it to their own servers. Has anyone been told by their ISP that they are doing this? No? I didn't think so. Subversion of DNS, even for your own good, is not a good thing. This has the effect of controlling wherever you go on the internet. It is a good thing our ISP's know better than we do. Not!

I need your help here. I would like you to run some simple tests and report your results to me. I need you to run an NSLOOKUP or DIG to a specific name server on a specific zone that the DNS has not been made aware of. Using the zone for the query will cause any subverted queries to return non-existent domain (NXDOMAIN). If you have a few minutes please go to the following link on my home page and give it a try. Go to <http://www.paulparisi.com/queryproject> and input your findings. Once we get a critical mass we will start to publish the report.

Originally published on 20090625

at http://www.circleid.com/posts/just_say_no_isp_subverting_dns_queries/