Configuring DNS to help protect your Home IT

Have you ever seen a picture of an old fashioned telephone operator? The operator played a critical function in establishing a global telephone network where any phone could talk to any other phone. When a person wanted to make a call, they connected to the operator and the operator would either connect the person directly to the other party or connect through other banks of operators. Without this ability to switch and connect physical wires together, phones would never have worked.

All of that has been automated now. When you dial a phone number, computers figure out the smart way to connect your conversation with the right party.

The Internet only works because it has a similar automated switching system. This system is orchestrated by something called DNS (short for Domain Name Service). Every device you have, indeed, every device on the Internet, uses DNS to determine how to route information to other devices.

When you buy Internet service for your home or small business, your Internet Service Provider automatically configures a DNS service for you. And when you authorize any

device to join your home network, your network and your device are smart enough to automatically configure themselves to use your ISP's DNS service. It all works so smoothly that you almost don't need to think about DNS at all.

But it turns out there is good reason to consider how you configure your DNS. If you configure it correctly, it can be an important part of your defense, helping keep bad guys and their software from attacking your systems.

Consider for example, the example of the old-fashioned phone operator. What if you were receiving a call from someone you do not know, and before connecting the operator gets on the line with you and says "Based on our historical records, the person calling you has a record of conducting fraud and they are probably going to try to deceive you." That would have been a nice feature back in the day.

If you configure your DNS properly, you can put features like that, and far more, at your command. Depending on which DNS features you want and which provider you select, you can use a managed DNS service to speed up your web browsing. You can also use it to make customized filtering decisions for your home system (for example, you can tell it that no one should have access to certain types of sites). You can also use managed DNS to prevent viruses and other types of malicious code from communicating with their bosses (their control servers), which can help reduce the chance that your information will be stolen from malicious code.

Also, consider again the example of the telephone operator. Imagine an operator who was working with a criminal. A good caller might dial the operator asking to be connected to the bank, and the malicious operator might really connect the caller with a criminal group for bent on fraud. Traditional DNS has weaknesses like that. With certain types of DNS attacks an adversary can make you think you are going to a favorite website but can re-direct you to a bad one, perhaps to steal your login info or to download malicious code. This is another very important reason to use a managed DNS service.

There are cautions to consider when selecting a DNS provider. Some DNS providers collect information from you in ways that may creep you out. For example, if you select the free DNS service from Google, although there are privacy protections, they will be aggregating even more data on you and your browsing habits. It is free and offers protection and is backed by a company with incredible engineers, but you will give up some info you might want kept private.

Four options for your managed DNS service are: Google Public DNS, OpenDNS, GlobalCyberAlliance, and Verisign DNS.

Google Public DNS: Google is doing a great service for the world with this free DNS resolution service. This will speed up your browsing, improve your security, and get you results with no redirection. But guess what? They get something out of it too. They get data.

OpenDNS: Now part of Cisco, this firm was early in the home user market and is now growing among Cisco clients. Free and very low cost options for home users. Makes browsing faster

and more secure. If you want the best malware protection you pay a small amount ($20.00 per year covers the entire household) and add software on your roaming devices.

Global Cyber Alliance: The Global Cyber Alliance (GCA), in partnership with Packet Clearing House (PCH) and a consortium of industry and non-profit contributors, is building a global anycast open recursive privacy-enabled DNS infrastructure. This reduces risk, speeds browsing, and since it is being fielded by a non-profit there is no collection of personally identifiable information like some other providers. It is in a pilot status. Contact GCA for more info.

Verisign: Verisign Public DNS is a free DNS service that offers improved DNS stability and security over other alternatives. Verisign respects privacy. DNS data and other PII is not sold or shared or used to serve you ads.

Now how might you implement DNS at home? Each of those services is going to give you very easy to follow tips for using them, and the methods are really the same for any DNS provider you use. You will change the DNS entries on your home router, and you will also change the DNS settings on your mobile devices and computers. It is all quite easy.

Tips for Changing Your Home DNS:

- Routers all have slightly different instructions but you should easily be able to find a section for DNS. It is a best practice to note what the DNS settings currently are (just in case you want to change back). But when you are ready simply change to be the DNS numbers of the service you have decided to use (for example, for Verisign, use 64.6.64.6 and 64.6.65.6).
- For mobile devices, look under your Wi-Fi settings and update the DNS entries there.
- For MacOS devices, go to settings and select "Network". Select a network interface from the sidebar and click advanced. Click the DNS tab and click the + button to add a new DNS server. Then enter the new DNS numbers.
- For Window devices click the Start button and then control panel. Under Network click View network connections. Then right-click the connection you want to change, and click properties. Click either IPV4 or IPv6 and click properties. You will see where to enter the DNS numbers.

Configuring your DNS is by no means the only step to take at home (we also strongly recommend using multi-factor authentication on all your accounts and using a good password manager). However, if you optimize your DNS configuration you can reduce your overall risk.

Do you have questions, comments or suggestions on DNS configurations for security? Get in touch with us at

CognitioCorp.com

Cognitio Cyber Leadership

Cognitio is a strategic consulting and engineering firm enabling companies to more effectively maximize the impact of technology investments and reduce overall digital risk. Cognitio helps clients improve their defenses by:

- Independent assessments of security posture leveraging best practices and our Cyber360 framework
- Providing executive-level “CISO-as-a-Service” support
- Campaign plans and technology assessments enabling optimization of security spend

Roger Hockenberry

CEO, Cognitio. Background in cyber security in the IT and Healthcare industries and in the Intelligence Community.

Bob Gourley

Partner, Cognitio. DoD and Intelligence background. Cyber Intelligence assessments across multiple industries.

David Highnote

Partner, Cognitio. Background in strategic consulting and cyber assessments in multiple industries. Media experience.

Bob Flores

Partner, Cognitio. Former CIA CTO. Background in enterprise tech and cyber security assessments.

Chris Ward

Senior Analyst, Cognitio. DoD and consulting background. Strong in enterprise IT including applying right tech to mission needs.

Chuck Hall

COO, Cognitio. Background in Healthcare IT and cybersecurity as well as business leadership.

Crystal Lister

Lead Analyst, Cognitio. Background in all-source cyber threat and counterintelligence analysis in the Intelligence Community.

Cognitio analysts include Dan Cybulski, former head of high performance computing for the U.S. government, and Leslie Wilfong, highly regarded data scientist.

CognitioCorp.com

Copyright Cognitio Corp March 2017

All questions and enquiries regarding this paper should be directed to:
Bob Gourley
Partner and Co-Founder
Bob.gourley@cognitiocorp.com