Use OpenDNS to surf safely with these tricks

By Becky Waring on July 9, 2009 in Top Story

By Becky Waring

Windows Secrets editors frequently recommend OpenDNS, a free service that blocks dangerous sites so you can browse the Web securely.

Unfortunately, OpenDNS has a few tricky gotchas for the unwary, but most of the problems can be solved if you set up an account and take advantage of a few tweaks.

In her June 11 Top Story, WS contributing editor Susan Bradley described how to use OpenDNS to help combat malicious Web sites. In essence, you quit letting your ISP's server convert domain names (like Google.com) into IP addresses (74.125.45.100) for your browser. When you type a domain name, the conversion to an IP address goes through OpenDNS instead.

This simple substitution of one set of DNS servers for another should eliminate the intermittent server outages that many broadband subscribers experience. OpenDNS uses a global network of servers that can be redirected in case of overload or failure. The service's main page shows the servers' locations in the U.S. and Europe. In addition, OpenDNS claims to resolve requests quicker than the DNS servers of most ISPs, which means pages should load faster.

However, the real power of OpenDNS — and the reason Susan and other experts recommend it as a defense against Web-based malware attacks — lies beyond mere name-to-number serving.

By filtering the URL requests that come to you through its servers, OpenDNS can block your browser from surfing to phishing sites and other kinds of undesirable content. The service also corrects typos you make, such as **google.cmo,** and lets you create URL shortcuts for quick access to the sites you visit most often.

OpenDNS is currently beta-testing a new SmartCache feature that loads the last known-good address for a Web site, even if its nameserver is offline. This kind of outage can happen due to distributed denial of service attacks, for example. This spring, Amazon.com and other big-name sites were unavailable for several hours due to this type of assault, as described in ZDNet's Between the Lines blog. With SmartCache, OpenDNS users can access these sites even though other Internet users cannot.

With such a simple premise, OpenDNS sounds great, right? Unfortunately, some people — including several WS readers who wrote in after Susan's story appeared — have had problems when attempting to use the service.

The correct way to set up OpenDNS

The issues our readers and other OpenDNS users report are due mainly to an incomplete or incorrect setup of the service. Many articles that recommend using OpenDNS say only that you should replace the DNS servers in your computer or router with two OpenDNS-controlled IP addresses: **208.67.222.222** and **208.67.220.220.** These articles, while meant to help users, fail to tell the rest of the story.

A simple IP address replacement is indeed all most OpenDNS users need to do. Full control of your OpenDNS experience, however, requires that you create an account on OpenDNS.com. Without an account, you're stuck using the default preferences, which may not work for your setup. For example, you may not be able to access a VPN (virtual private network) or Windows Home Server without changing your account preferences.

Similarly, you can't take advantage of OpenDNS's powerful filtering options without establishing an account. By default, OpenDNS uses a so-called PhishTank list to block phishing sites; the list is maintained by OpenDNS itself. But if you're a parent or employer who also wants to block sites in such categories as pornography, illegal downloads, social networking, or video sharing, you need to do so by configuring your account preferences.

To set up a free account, simply go to OpenDNS.com and sign up. You must also change the DNS servers in your router to the two IP addresses mentioned above. Instructions for doing this on most routers can be found on the Use OpenDNS page. Once your account is confirmed, sign in at the OpenDNS site and open the Dashboard to change your account preferences. (See Figure 1.)

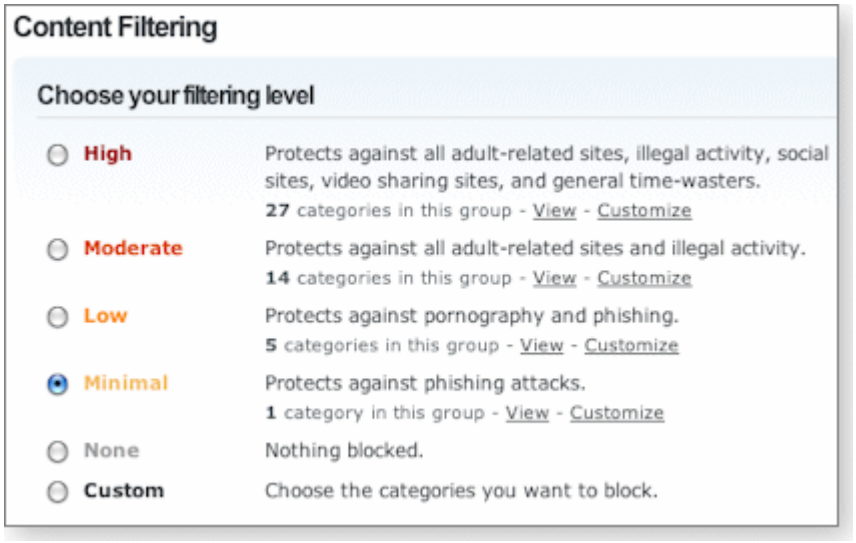

Figure 1. Customize your OpenDNS settings via the service's Dashboard.

To customize OpenDNS for a typical home PC user, you would first add your home network using the Networks tab. By configuring OpenDNS in your router and adding your home network, you can protect ***all*** your computers and network devices — including smartphones that connect via Wi-Fi — with the same account settings. If you use multiple networks, you can add them all under the same account.

When you travel, you can change the DNS settings for your laptop's Wi-Fi and Ethernet adapters to connect to OpenDNS directly, rather than relying on your home network to make the connection. Instructions for Windows, Mac, and Linux computers are available on the OpenDNS Change DNS settings page. (It's fine to use both computer and router OpenDNS at the same time.)

Next, click the Settings tab to choose and customize your Web-filtering preferences. I have mine set at the second level, **Low,** which blocks phishing and pornography sites. Parents may want to choose a higher level of protection. You can also create custom lists of allowed and blocked sites, regardless of the level of protection you select.

Accessing the real OpenDNS mother lode, however, may be a bit more difficult for the typical user to figure out. Click Settings, Advanced Settings. (See Figure 2.) This is where you can add your VPN or Web server, activate the SmartCache feature, and enable dynamic IP updating — which is particularly useful for travelers.

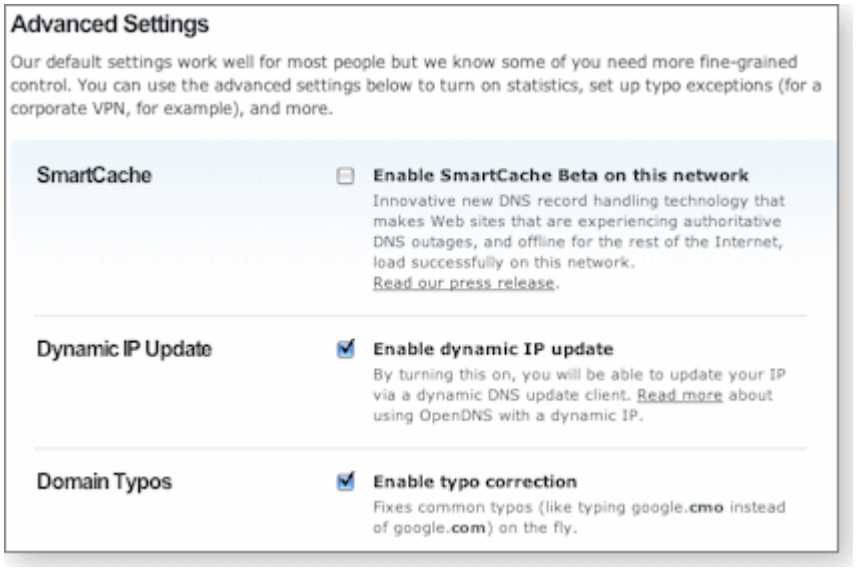

Figure 2. The OpenDNS Advanced Settings page lets you customize your use of the proxy service.

To reach a VPN or corporate intranet domain, or to access such resources as network printers and network shares, you have two options. For home networks, simply add a “Domain typo exception” in the name of your VPN server or network domain; for example, **vpn.*mycompany*.com.** Together with dynamic IP updating, this solves a problem with remote access and Windows Home Server.

If you’re already running a local DNS server such as Windows Server 2008 with Active Directory, your second option is to forward only external DNS requests to the OpenDNS servers and continue to resolve local domains locally. In this case, you update the external DNS settings to OpenDNS on your server, ***not*** in your router or client computers.

People who rely on a dynamic IP address from their ISP or who travel frequently can download and install the OpenDNS Updater, which is available on the OpenDNS Support page.

Putting OpenDNS to the speed-comparison test

Once you’ve got OpenDNS configured properly, it’s time to try it out. First, you can attempt to verify OpenDNS’s speed claims with the handy DNS Performance Test from Silverwolf’s Auditorium. Run the test on your regular ISP’s DNS servers and on OpenDNS’s servers.

In Northern California, where I live, the results confirmed some complaints of slowness by the alternative service. AT&T’s DNS servers, accessed via my standard DSL service, were twice as fast at resolving DNS requests as OpenDNS: 89ms versus 187ms.

While 187ms is a fairly good response average, the OpenDNS folks indicated that my results were atypical, especially since they have a server located near my house. When I asked several other Windows Secrets editors to run the same tests from their locations around the world, their results varied widely.

For example: In New Hampshire, Fred Langa got a test result of 132ms from the servers at his FairPoint ISP and 146ms from OpenDNS. In Colorado, Scott Spanbauer's Comcast connection registered 119ms compared to OpenDNS's 116ms. And in Phuket, Thailand, Woody Leonhard's TT&T MaxNet DNS served up 547ms against OpenDNS's score of 414ms. These results are virtual ties.

The bottom line is that your mileage may vary. I recommend that you run the same tests on your connection before committing to using OpenDNS. Even if you find a small performance deficit from OpenDNS, the minor slowdown should be evaluated against the security and reliability benefits OpenDNS can bring.

If you find a larger difference, this may argue against using OpenDNS from your area. In that case, you can also try DNS Advantage, a similar service from NeuStar. DNS Advantage is still under development but will soon be adding site-blocking and typo-correction services similar to those offered by OpenDNS.

NeuStar already has a large network of DNS servers for its paid, corporate UltraDNS service, so DNS Advantage is likely to become a big player.

Assessing readers' reports of OpenDNS glitches

As I mentioned above, some WS readers reported difficulties in using OpenDNS after Susan's story appeared. David Cagle complains that his ISP is blocking the service:

- "Here in Florida, with Comcast as my service provider, it's almost impossible to reach the OpenDNS Web site. After several days, I became suspicious and began doing some Web searches. Thread after thread of angry Comcast subscribers are all reporting that OpenDNS is either blocked outright or hobbled to the point of being useless."

While several readers reported problems when using OpenDNS with Comcast, Scott Spanbauer experienced no such difficulties when he tested OpenDNS over his Comcast connection. Further, OpenDNS CEO David Ulevitch assured me that "we have many millions of users in the U.S. and many of those are Comcast customers. We've had no complaints from them. We also know the Comcast DNS engineers reasonably well, and we know they

aren't doing any blocking."

It's likely that David's problems stem from his particular setup. (OpenDNS contacted David to try to help him out, but as of early July, he hadn't responded.)

Reader Ernie Mandoky warns of another potential problem related to OpenDNS use:

- "Windows Secrets readers who employ Windows Home Server should be warned that OpenDNS will not translate the server's IP address correctly and will prevent clients from connecting to the server through both [Recovery] Console and Remote Desktop. Backups will continue to function automatically, and you can even access the server by entering the server's IP address directly into the browser, but the Console will no longer connect."

As I described above, to protect a home network simply add a "Domain typo exception" in the name of your VPN server or network domain — for example, **vpn.*mycompany*.com.** Together with dynamic IP updating, this should eliminate problems concerning Windows Home Server and remote access.

Rick McLeod found that his system performance slowed to a crawl after he installed OpenDNS, and he concluded that his PC had become infected:

- "Because of following [your] advice on OpenDNS, I now have a browser hijack when I enter an invalid URL. It goes to their search page. I didn't ask for that and am having big difficulty getting rid of it."

OpenDNS isn't any kind of a hijack or exploit. Displaying a search box when a user types a domain name that doesn't exist is an OpenDNS feature. If a common error is made — such as typing **google.cmo** — the service just sends you to the correct page. If there's no easy match, however, OpenDNS directs you to a search page, which contains advertising that supports the service.

I feel this is a small price to pay for such a valuable free offering. This is especially true because most of the typos I make while using OpenDNS are automatically routed to the correct domain, saving me the hassle of retyping. Few Internet services as useful as OpenDNS are truly free. As long as the ads don't get in my way, I'm willing to make the trade-off.

UPDATE 2009-07-16: In his July 16, 2009, Known Issues column, technical editor Dennis O'Reilly catalogs reader suggestions on ways to improve the OpenDNS service.

SOURCE: https://windowssecrets.com/top-story/use-opendns-to-surf-safely-with-these-tricks/