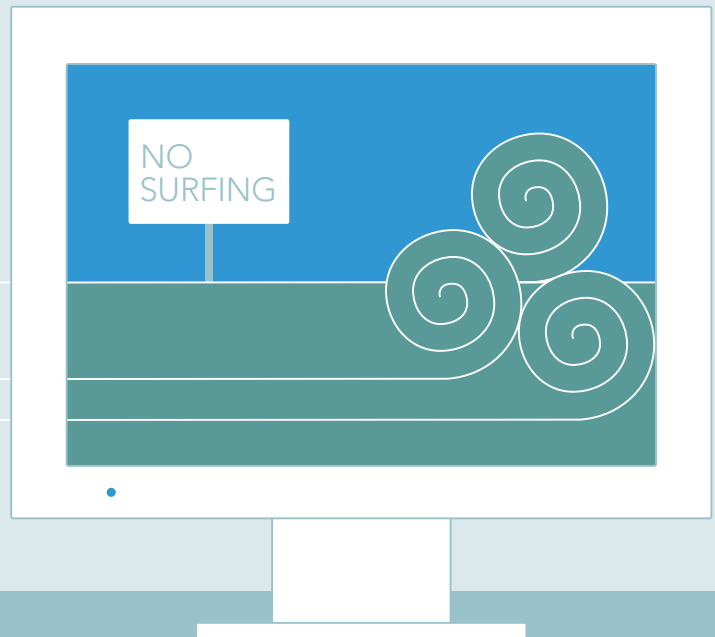


REDUCING IMPROPER INTERNET USE IN YOUR OFFICE: A QUICK, EASY AND FREE SOLUTION

In just a few minutes,
you can set up your computer
system to block Web sites
that aren't appropriate at work.



JAMES DOM DERA, MD, FAAFP

Walk into any family physician's office across the country and, regardless of the scope of practice, you will find some common tools: stethoscope, otoscope, blood pressure monitor, scale and so forth. But one more tool has become indispensable in our offices: the Internet.

While the Internet can be a powerful tool for gathering information and communicating with others, it can also be a great time waster and a temptation for both physicians and their staff. According to a survey conducted in 2007, the average employee wastes 1.7 hours of an 8.5-hour workday, with personal Internet use being the leading time waster.¹ In addition, inappropriate Internet usage can make computer networks more vulnerable to malicious attacks. Because of this, practices need a way to enable the legitimate use of the computer while blocking the unnecessary use.

Internet blocking software is widely available and use-

ful for this purpose. However, depending on the size of the office, it may cost hundreds to thousands of dollars per year and be difficult to manage. There is another quick, easy and free alternative: OpenDNS. OpenDNS allows an employer or computer network administrator to block selected Web sites while allowing access to others.

What's a DNS?

Web site addresses function very much the way phone numbers do. For example, if you want to call your neighbor, you must dial his phone number. If you don't know it, you either consult the phone book or call the operator.

The Internet works in a similar way. If you want to read the news in the morning, you might type "www.msnbc.com" into your Web browser and within a few seconds up pops the day's news. Humans think in terms of names and letters: msnbc.com, espn.com, aafp.org, etc.

THE AVERAGE EMPLOYEE WASTES 1.7 HOURS OF AN 8.5-HOUR WORKDAY, WITH PERSONAL INTERNET USE BEING THE LEADING TIME WASTER.



Web sites, however, are located by the number assigned to them, known as their IP address.

So how does a computer translate www.msnbc.com into an IP address such as 207.46.150.20? This is where a “domain name server,” or DNS, comes in. When you type the address into your Web browser and press “enter,” the name you typed in is sent to a DNS. The DNS is the Internet’s “operator.” It searches its list of Web sites for the IP address. If it cannot find the Web site, it sends your request to another DNS. This process continues until the IP address is found, and then you are connected.

The DNS used by your computer is usually picked for you by your Internet service provider. However, you can change this to any DNS you want. By doing so, you can take control over which Web sites you want to load and which you want to block.

How OpenDNS works

OpenDNS (<http://www.opendns.com>) allows you to limit access to certain Web sites either on one computer or on an entire computer network simply by changing the DNS setting. There is no installation necessary, and the process takes only a few minutes.

For example, if you simply want to change the DNS setting on a single computer using Windows XP, you would do the following:

1. Select Control Panel from the Start menu and click Network Connections,
2. Choose your connection (e.g., Local

Area Connection or High-Speed Internet),

3. Click the Properties button,
4. Select Internet Protocol (TCP/IP) and click Properties,
5. Click the radio button next to “Use the following DNS server addresses” and type in the OpenDNS addresses 208.67.222.222 and 208.67.220.220 in the Preferred DNS server and Alternate DNS server fields, respectively. (See detailed directions tailored to your system at https://www.opendns.com/start/windows_xp.php.)

I changed the DNS of our small, 10-computer office network to OpenDNS one weekend while in the office catching up on some work. The technical part was simple. Explaining the change to my staff was a bit more complicated. By the next Wednesday, I already had two complaints from office staff (and one from an employee’s son!) who could no longer access their favorite Web sites. I gently reminded them that office computers are for business use only, as many of the blocked sites were not appropriate for the office. Admittedly, even I have fallen victim to my own rules on occasion, usually when a friend sends me a link to a video on [youtube.com](http://www.youtube.com) (a site I have blocked at the office). I have to wait until I get home to view the video, or I just delete the e-mail, but these small inconveniences are outweighed by the many benefits of using OpenDNS.

Advantages. The major advantages of OpenDNS are its speed, security and customization. OpenDNS maintains one of the largest lists of Web sites. This list, known as a cache, allows OpenDNS to quickly serve up a Web site, rather than having to search for an IP address. If you create a free account with OpenDNS, you or your network administrator can then control the Web traffic on your

You can block selected Web sites on the computers in your practice without having to buy or install new software.

To connect to Web sites, your computer relies on a domain name server (DNS), which is usually selected for you by your Internet service provider.

By selecting a DNS such as OpenDNS, you can control which Web sites are accessible in your practice.

About the Author

Dr. Dom Dera is a family physician in private practice in Fairlawn, Ohio. Author disclosure: nothing to disclose.



Article Web Address: <http://www.aafp.org/fpm/20090300/20redu.html>

practice's computers. With one click, you can block all known adult sites. Another click will block all known phishing sites, which are sites that fraudulently attempt to steal personal and financial data by appearing as legitimate Web pages. (OpenDNS gets its list of adult sites from St. Bernard's iGuard service and phishing sites from PhishTank.) If a computer user tries to visit one of those sites, they are redirected to a warning page from OpenDNS and prevented from going further. This warning page can even be customized with a graphic and personalized logo.

Additionally, specific Web sites can be added to a "block list," and those will also be inaccessible. For example, I have myspace.com and facebook.com, among others, on my block list. Anyone in my office trying to visit those sites will be redirected to the OpenDNS warning page (complete with my corporate logo and a personalized warning from me). I've also blocked a number of advertising sites (doubleclick.net being the most common) so Web pages won't display tempting and time-wasting ads. On the other hand, adding a Web site to the "white list" ensures that it will *never* be blocked.

OpenDNS offers many other useful features. For example, shortcuts can be set up to eliminate the typing of long, hard to remember Web sites. Typo correction will automatically correct misspelled Web sites (e.g., www.aafp.org will become www.aafp.org). OpenDNS also provides a log of sites requested by your employees, so you can get an idea of what types of sites they are visiting or trying to visit.

Disadvantages. OpenDNS makes money through advertiser links (the same way Google and Yahoo do). For example, if a user types in a Web site not known to OpenDNS, a search

page will come up and the top few links will be labeled as "Sponsored." These advertiser links could be distracting and lead to further surfing.

Additionally, OpenDNS only works with known Web sites. It will not stop users from visiting a Web site that is not known to iGuard or PhishTank, unless you manually add them to the block list for your account. It will also do nothing to stop users from using instant-messaging clients, downloading software or using peer-to-peer file-sharing applications (such as KaZaA, an application used for sharing MP3 music files). Using a good and updated anti-virus program is still mandatory.

One big disadvantage to OpenDNS is that it affects only DNS requests. If the user happens to know the IP address of a Web site, then the DNS is bypassed altogether. For example, OpenDNS will stop a user from visiting playboy.com. It will not, however, stop a user from visiting 216.163.137.3 (Playboy's IP address). A knowledgeable and determined Internet user can quickly find the IP address to any site and completely override the security; however, the Web site would still show up in visit logs. An employer could add IP lookup sites to the list of blocked sites, but this could quickly turn into a cat and mouse game.

Finally, the OpenDNS service is only available to those with permission to change the network server settings. Without network administrator privileges, a physician would be unable to take advantage of OpenDNS.

A simple solution

Internet traffic management is an important part of every physician's computer network responsibilities. Sophisticated and expensive computer programs are available to help users accomplish this. An easier and free alternative is

to change the computer or network's domain name server to OpenDNS, which will allow exquisite control over allowed and prohibited Web sites. Set up is quick and easy, and the results are instantaneous. **FPM**

Send comments to
fpmedit@aafp.org.

1. Employees waste 20 percent of their work day (press release). July 25, 2007. Available at: <http://www.salary.com>. Accessed Jan. 14, 2008.

■
With one click, you can block access to all known adult Web sites and phishing sites.

■
You can also block access to sites such as Facebook or YouTube, which can be time wasters for staff.

■
OpenDNS is free to users but makes its money through advertiser links, one of several disadvantages.

OTHER FREE DOMAIN NAME SERVERS

This article focuses on OpenDNS because the author has experience using it. Other free DNS services include the following:

DNS Advantage, <http://www.dnsadvantage.com>

ScrubIT, <http://www.scrubit.com>

TreeWalk DNS, <http://treewalkdns.com>