Web filtering keeps you a little safer

By Susan Bradley

Web-filtering services can provide additional security and protection from malware.

Several vendors now provide this valuable service.

Either you've heard the stories or you've experienced it yourself: a fully patched Windows machine gets infected by rogue-AV malware (a virus disguised as an antivirus app). Before anyone realizes that the "AV scanner" that popped up on the screen is an AV scam, the damage is done — and hours or even days are wasted removing the infection and repairing Windows.

In most cases, PC users who acquire this type of contagion share some of the blame. They make the mistake of clicking a malicious Web link — in an online search result, an enticing image on a seemingly innocent webpage, an ad for some free product, an e-mail, and so on.

Getting infected is especially annoying when you thought you'd fully protected yourself by regularly patching Windows, applications, Flash, Java, and browsers — along with your antivirus software.

If you're wondering what else you could possibly do (short of pulling your connection to the Internet), I recommend adding Web-filtering services offered by DNS providers.

DNS providers offer free, personal Web filtering

Whenever your PC connects to an ISP, the company updates your gateway/router with the information it needs to connect with the ISP's Domain Name Services (DNS) servers. (DNS is the process by which numeric website addresses are translated into website names you can understand — such as **windowssecrets.com.**) Along with DNS, some ISPs (such as Comcast) include Web filtering — also called content filtering — for additional security.

Setting up Web filtering lets you control what sites can be visited through your local browser. Good Web-filtering controls allow white lists (sites that should always be accessible — such as **windowssecrets.com**), black lists (banned sites), and category-based filtering. Apps that establish parental controls over Internet sessions typically use Web filtering. (In extreme cases, Web filtering is used by repressive governments to limit the sites their citizens can visit.)

If your ISP provider doesn't offer Web filtering, you have another option. You can switch your DNS connection settings — either within Windows or on your router — from your ISP's DNS servers to a third-party DNS provider.

Although several vendors provide this service for home and small-business users, OpenDNS is probably best known. It offers both a free service and a Home VIP solution that costs U.S. $19.95 a year. This paid solution (more info) can display charts and graphs of sites visited from your home computers.

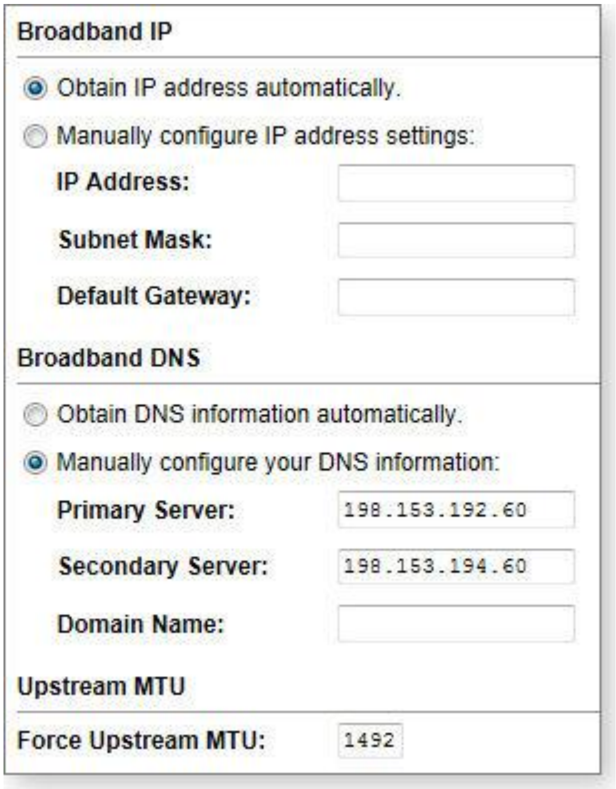
Making the switch is relatively easy, as long as you can access your operating system's network properties or your router's setup utility. OpenDNS provides simple instructions on its site.

Another option is Symantec's Norton ConnectSafe (site), which uses DNS-based filtering to block suspect sites. Like most content-filtering services, ConnectSafe uses site categorization, such as pornography, crime, gambling, and so forth. The easy-to-set-up service has three levels of filtering:

- **Policy 1:** This base-level filtering blocks malware, phishing sites, scam sites, and Web proxies. For this level, set your DNS entries to **192.153.192.40** and **198.153.194.40.**

- **Policy 2:** Medium filtering adds pornography blocking. Set your DNS to **198.153.192.50** and **198.153.194.50.**
- **Policy 3:** This stringent filtering blocks a host of sites that Norton ConnectSafe deems not family-friendly, filtering for mature content and other family-unfriendly content. To choose this filtering, use **198.153.192.60** and **198.153.194.60** (shown in Figure 1).

Once ConnectSafe is set up, you can visit its "Configure Router" page and click the "Test Norton ConnectSafe" button to ensure filtering is enabled.



Broadband IP

● Obtain IP address automatically.

○ Manually configure IP address settings:

IP Address:

Subnet Mask:

Default Gateway:

Broadband DNS

○ Obtain DNS information automatically.

● Manually configure your DNS information:

Primary Server: 198.153.192.60

Secondary Server: 198.153.194.60

Domain Name:

Upstream MTU

Force Upstream MTU: 1492

Figure 1. Setting up Norton ConnectSafe in a 3Wire DSL modem

Norton ConnectSafe does not provide custom white/black listings. And with just filtering by category, there's no guarantee that all objectionable sites or content will be blocked. Also, using the strongest filtering setting might block sites you want to visit or that aren't objectionable to you. Before committing to ConnectSafe, test that the filtering isn't too restrictive.

Another consideration: If you change DNS settings in Windows, it applies only to that machine. If you change settings in a router, it applies to all systems that connect to the Internet through that router.

An alternative to ConnectSafe is Dyn's Internet Guide, which also uses site categorization. Internet Guide's filtering options are more flexible than Norton's; it offers predefined filter lists, category selection, and custom site white/black listings. As noted on its info page, you use **216.146.35.35** and **216.146.36.36.**

Web/content filtering for small businesses

Small businesses now have fewer, or less attractive, DNS-filtering options. Beginning March 15, OpenDNS changed its DNS plans and no longer offers low-cost filtering for small businesses. Subscribers must choose between the Premium DNS plan (info page), which does not include filtering, or the OpenDNS Enterprise plan, which ***does*** includes filtering but at a significantly higher cost. The quote for my business was $1,500 per year to protect 1–50 users. The price increase prompted quite a bit of discussion on an OpenDNS Forums posting that announced the change.

For now, Norton DNS for Business is still free, as noted in a February post. DynDNS also offers free filtering for small businesses (info page). I'm evaluating both these offerings for my business, given the high price tag for OpenDNS.

When it comes to anything offered for free, one has to ask: Where's the catch? There has to be something of value for the service providers. Most likely, both entities use the filtering process to gather information they can apply to their core business offerings. Symantec, for example, sees what websites customers visit. As noted on its privacy policy page, any data it might collect from site visits is discarded after two days. (It cannot view content sent over SSL connections.)

It might be cause for concern that an entity providing security solutions could see the sites you surf to. However, most — if not all — sensitive information should travel over SSL connections. So I'm OK lowering my paranoia a bit to ensure I continue to have objectionable websites filtered and blocked.

I'm convinced that using filtering has helped keep my home and small-business computers free of rogue antivirus and other malware posted on malicious websites. With so many threats coming from browser use, I see this as a security win — and not a privacy issue.