

TechTalk: How can you insure your company web browsing remains safe?

By **MJ Shoer**

September 18, 2009 2:00 AM

I'm sure you are familiar with the problem: You or someone you know is browsing the Internet, seemingly on a safe Web site, and then the pop-ups start. Somehow, you've gotten infected with spyware or worse.

Just this week, users of the New York Times Web site experienced problems caused by a malicious banner ad that infiltrated the site. This fake ad caused a window to pop up on users' computers, warning them they had a virus and instructing them to download software to fix the problem. Fortunately, most users know a pop-up like that is fake and likely a lure to get you to download software that will really cause problems, not the least of which may be identity theft.

If sites as reputable as the New York Times can be infected like this and cause problems for legitimate visitors, what can you do to protect your network?

The obvious perimeter security measures need to be in place. A robust hardware firewall appliance that will inspect traffic coming in and leaving your network is a must. Appliances such as these allow you to specify very specific rules as to what may come and go and therefore protects the computers behind it. A centrally managed anti-virus and anti-spyware solution is another must. Everyone is familiar with anti-virus software and should be with anti-spyware software as well. These need to be continually updated, tuned and monitored to ensure they provide the protection they are intended to. Many threats today will attempt to disable these defenses, so keeping vigilant watch on their operations status is imperative. Centrally managed software firewalls on individual computers are very helpful and should be a standard these days.

Those are some of the very obvious measures even the most basic computer network should have in place. However, there are some additional services that complement these, to help ensure a safer network.

The Domain Name System, or DNS, is the Internet service that translates the common names of Web sites, like www.nytimes.com, to the corresponding Internet address, or IP address, where the Web site actually exists. Many threats will attempt to overtake the DNS services that your network relies on to redirect you to fake or malicious Web sites that try to pass themselves off as the real thing. Using a DNS filtering service is a simple and very effective way to protect against this and ensure you are really browsing to the sites you think you are. More advanced services will also provide protection against known sites and threats, continually monitoring the Internet and updating their databases of malicious sites, with the goal of only allowing you to surf the safe places.

There are also traffic shaping devices that allow you to manage your Internet connectivity by restricting where people can go, or minimizing the amount of Internet bandwidth allowed to be used for certain types of sites. These types of devices allow you to restrict access to certain places on the Internet or prioritize sites based on the value to the business. For example, you may want to ensure your finance department can get to all the banking and financial sites they need to use, while minimizing or preventing outright the use of fantasy football sites, to ensure work takes a priority over play.

Some of this definitely skirts the edge of censorship and can be a bit reminiscent of "big brother," but properly implemented with the right intention, they can help ensure your use of the Internet remains as safe as possible.

Regardless of what defensive technology you put in place, and I have only touched on a few in this article, the final line of defense is also the person. There is no substitute for educating your computer users on proper and safe use of the Internet. This will continue to be a highly important part of managing your personnel, ensuring they are properly trained on safe computing to ensure your business remains safe in our highly connected world.

MJ Shoer is president and virtual chief technology officer of Jenaly Technology Group, Inc., a Portsmouth-based outsourced IT services provider. He may be reached at mshoer@jenaly.com.