

Safe browsing in today's Internet: Can it be done?

**Paul Locander, Manager, Network Systems & Support
DelCor Technology Solutions**

For all the promise that is the Internet today, it is also very much like taking a stroll through Dodge City in the late 1800s where you take your life into your own hands. Only in this case it's your computer's life, your online identity, and your bank account that you offer up for sacrifice the moment you start up your browser. Where else can you be held up, solicited, bullied, embarrassed, lied to, cheated, maligned and addicted all without having to leave the comfort of your own home or office?

What's more, malicious Web sites are a growing threat—the electronic equivalent of stepping on a hornet's nest and unleashing thousands of stingers specifically designed to infect your computer. Microsoft, Apple, Adobe, and others frantically release patches on a regular basis to protect us from the killer bees, but the hornets are always one flutter ahead.

For the software providers, it's commercial whack-a-mole. For consumers, it's an endless assault on our productivity, security, and wallets. It's gotten so bad that even misspelling a URL could open your computer to being taken out at the knees.

In search of a cure

PC users running on the Microsoft platform generally get the worst of it, an honor granted to them based on Microsoft's market share and the historically porous state of its product line. But, fear not; Apple, Adobe, and even your cell phone are starting to catch up.

While antivirus manufacturers continue to crank out products designed to protect our systems—and most are putting forth a valiant effort—our Windows computers are still getting infected. Until now, there's been no way to prevent it outside of unplugging your computer from the network, or simply abstaining from the internet.

With all the technology at our fingertips, isn't there a fearless way to hop onto the Internet without having to strap on a pair of six-shooters?

There is ... with virtualization.

'Virtual browsing'

An ideal way to safely browse the Internet is to separate the PC as much as possible from the browser—in essence, to browse on a separate computer.

For most of us, having a separate computer on our desk for browsing

Checklist for creating a virtual browsing environment

- One Windows-based PC
- Ubuntu Linux
- Sun VirtualBox
- 60-90 minutes
- Technical skill

isn't a very practical solution. However, by leveraging desktop virtualization, you can do just that. And you can do it easily.

The test

To test this theory, I installed the latest version of Ubuntu's Linux in a virtual environment on a Windows 7 PC using Sun Computer's free download of VirtualBox, an open-source virtualization application that works on Windows XP and up, providing hosting environments for a multitude of operating systems, including Windows and Linux.

Why did I choose Linux as opposed to, say, running another version of Windows virtually? First, malware, Trojans, and viruses are not generally geared to attack the Linux operating system in mass, so even going to a malicious Web site armed to the teeth to take out a Windows PC running Internet Explorer will have no effect on my new browsing solution. Second, both solutions are free, so I avoid issues specific to licensing (although Microsoft does make provisions for virtualization for clients subscribing to the Software Assurance program). The solution was low-cost and as attack-resilient as possible.

After going through a short, basically problem-free installation, I created a virtual machine using a pre-installed template for Ubuntu, and within about an hour I had Linux up and running. Voila! Two computers for the price of one! By leveraging the seamless technology that comes with VirtualBox, I have the ability to move across both operating systems and the Linux-based web browsers with ease.

So, does it work?

For general use, my new 'virtual browsing' environment has so far proven to be a good solution, both in performance and security. Even if I do come across a malicious Web site, there isn't much to infect since the browser is running on Linux; in the off-chance that the operating system gets attacked, the damage is contained within the guest OS, which can easily be recreated (or even restored from a snapshot in less than two minutes) if need be. A much more attractive option versus having your computer eradicated, or having to reinstall your operating system and applications.

Cut-and-paste is a snap and mouse control is seamless between the Windows host OS and the Linux guest OS. (There's a post-installation step that you need to do to get that to work, but even that is relatively easy.) You can even share files between the two operating systems.

That's the good news.

“Yes, Virginia. You can protect your PC from malware attacks ... with ‘virtual browsing.’”

The not-so-good news is that there are limitations to this solution. The primary one that I've come across is interacting with sites specifically coded for Internet Explorer and/or for browsers on the Windows platform. Fortunately, those sites are relatively safe, but I could still run into trouble if I were to venture beyond them.

Some technical skill is required to install this virtual browsing environment; but, as a clean, low-to-no-cost solution for safe-browsing, this is one to consider.



8380 Colesville Road, Suite 550
Silver Spring, MD 20910