the Marcus LETTER

WHY YOU CAN TRUST SYMANTEC

Virtually A New Program Every Day

No problem in computers is more pervasive than the attacks, via viruses, worms, phishing and the like, produced by crooks, villains, wise guys, and adolescents of all ages, from what seems like every country of the world. How easy it is to take for granted the intercession of the virus hunters – Symantec, MacAfee, Trend Micro and others. They seem to work in secret witches' caves, brewing up whatever potions they brew up to divert the villainous stuff thrown at us by the bad guys. Just like that. Hah!

Recently I had the privilege to attend a two day seminar, run by some very senior Symantec engineers, analysts, and technical executives, to assist those of us who review Symantec and other computer products. They brought in the senior people from Santa Monica, Austin, and even Ireland.

Why does Symantec have so many technical locations around the world? So that they can take advantage of time zone differences to monitor intrusions from anywhere around the clock. It's a vast 24 hour, seven days a week, sweep. It's why they're able to develop antidotes within 48 hours or less.

A lot of it was technical -- more than I can handle, or that most of you might be interested in. But what is interesting – and important – is the scope and depth of what they actually do to protect us. It's awesome. It would put comparable consumer protection laboratories to shame, including the likes of the U.S. Food and Drug Administration.

Essentially, they covered malware testing methodologies, firewall and intrusion prevention systems, performance benchmarking, anticrime-ware testing, and anti-phishing. Some examples of the lengths to which they go include exploring network attack scenarios, developing firewall and intrusion prevention systems, performance benchmarking, anticrime ware testing, and antiphishing systems. It's an ongoing and persistent process.

The Symantec labs are constantly developing procedures to detect and immobilize antivirus and antispyware products, to develop firewalls that reflect user scenarios, even as they develop stronger

and more sophisticated firewalls. They work constantly to improve system impact, in terms of boot and resume time, memory utilization, and installation time. They constantly seek better transaction security technologies. And even sort out and fight phishing technologies. It's a lot of very serious people working some very serious technology, all for a relatively painless interface with the consumer that keeps our stuff as safe from intrusion as is humanly possible.

While the two day session was a course in how to evaluate security software, it was also an awesome lesson in the range of activities pursued by Symantec's technical staff. It's useful to remember that the variety of attacks on internet users is overwhelming, with new and innovative attack strategies developed every day. As one virus or worm is stopped, new ones spring up. Symantec, however, is more than just a software developer who designs a program and walks away until the next iteration is developed. Symantec is dynamic, adding new protections as the need for them surfaces, which can be many times a day. The world of the internet transgressor covers, it seems, any country that has electricity for some miscreant to use to run a computer.

While it's likely that Symantec's competitors function in much the same way, it's not difficult to see why Symantec is the leader in the field. It's a war, and Symantec is in the front line. Glad to see it.