**Protection On The Internet**

Some years back, and I don't know why or how I'm remembering this, but there was an interesting Star Trek episode. The crew had landed on a planet that claimed to be so advanced that they could avoid world wars. They accomplished this by using a randomly generated lottery of sorts which consigned a certain number of people to extinction. This grim lottery prevented mass destruction and only took out a small portion of nation's populations in a "fair way" to the plant's inhabitants.

What mystified the Enterprise crew is why they couldn't think of something else that would not only preserve the landscape and architecture and the people themselves.

What these planet inhabitants were doing was a sort of virtualization. A similar war where people in a "civilized way" would limit their destruction to a few. If your number came up, despite how few had to die, it was bad news.

Nowadays, virtualization is all the rage. Virtual servers save lots of hardware money. Sitting at home, I can Citrix into my work server and I can virtually be at work. Everyday could be a dress-down day.

I wish.

Yet we wonder if there is a way we could virtually surf on the internet and not pick up any of the malware from bad websites and crooks who probably look, in real like, like the ancient and evil angular-faced Cardasians.

You already know you've got to have ❶Antispyware ❼ Antivirus and ❸ a Software Firewall running on your computer to spend time on the internet. Unfortunately, it's gotten worse! You can go to a website (or be taken to a website by having clicked on something in an email) and unknowingly have viruses and spyware loaded on our computer. This brings us all to a new level of aggravation . It's too bad the government can't go after these people who are costing us all this money and time. To do so, though, they would have to track them down on the servers they use in South East Asia, China and remote parts of who knows where. The way the economy is going, they're not likely to make the investment.

In addition to getting unwanted software from bad websites, we all have internet friends who forward us stuff that has been forwarded to them. Fact is that of all the hundreds (maybe thousands) of emails we are sent, many contain viruses, Trogan horses, Worms and other hidden destructive programs. The Buffalo


Urban League uses MXLogic as its email filtering system. As of mid December 2008, of its nearly 400,000 incoming emails, 71% of them were denied. 595,082 were spams, 1,177 contained viruses, 4,771 were quarantined.

Then there are the "social engineering" emails that graciously ask us to click on something to benefit starving or homeless people. We are kind people so we want to but we get Zapped and have to reformat our hard drives.

**Here's help.** It's a great safeguard that seems well worth the $29. It's called *ForceField* and it is marketed by ZoneAlarm (*which happens to make one of the oldest and most robust software firewalls around*). It works like this.

When you go on the Internet, it automatically creates a pretend computer that exists in the temporary memory of your computer. Instead of your computer being exposed to the Internet, it is this pretend computer (or "virtual") PC. If you unknowingly land in a bad website that loads stuff on your (temporary) PC, you don't have to worry. When you close your Internet session, that temporary (or virtual computer) disappears, along with all of the spyware that may have been loaded on it without your knowledge.

I've been using and recommending *ForceField* for several months and have it installed on all of the PCs in our home. You can get it from:

http://download.zonealarm.com/bin/forcefield_x/index.html

Some of you also are familiar with Tor Project (see: http://www.torproject.org/) . It is a free virtual internet browser but requires the running of companion applications *Vidalia* and *Privoxy*. The *ForceField* tool, however, lends itself to much wider audiences who may lack the wherewithal to venture very far into virtualization.

➲ *Philip Siddons*