



ELEPHANT BOY COMPUTERS

3229 W. Sample – Fresno, CA 93711

Phone/Fax (559) 435-1224

www.elephantboycomputers.com

Don't Panic!

TOO MUCH SECURITY

We all know the old saying "you can never have too much money or be too thin", but can you have too much security? Absolutely. In the last month I've had two computers in the shop from different clients. The complaint in both cases was that the computer couldn't get on the Internet or Internet access was unbearably slow, they couldn't get email, and even off the Internet Windows was so sluggish that it was basically unusable. Classic case of malware infection, yes? No.

In both cases, each computer owner had installed multiple firewalls, multiple antivirus programs, multiple antispyware programs, and had set the security "immunization" features of all those programs to "High" without really understanding what they were doing. And although that was bad enough, they had also chosen the most bloated, problematic, resource-hogging, and invasive security programs out there. Major culprits with these characteristics are products from Norton (Symantec), McAfee, Zone Alarm, and Webroot SpySweeper, to name only a few. No wonder those computers performed so badly and couldn't get to the Internet - their owners had unknowingly crippled them in the name of "security".

And even though they had piled on all this "security", some of the programs used were obsolete, other applications that are avenues for attack (Java, Adobe Reader) were not updated, and Windows itself was not patched to the latest Service Pack. The machines were also jammed up with unwanted programs preinstalled by the computer mftr., all running in the background.

This is typically what happens when someone thinks he knows a lot about computer security and enjoys tinkering - a perfect example of "a little knowledge is a dangerous thing". Once I removed all the cruft and did basic maintenance and optimization, both computers ran sweetly. Here's how to do it right (and what I do on my own Windows machines):

a. Install and keep current one antivirus. I recommend NOD32 or Kaspersky for commercial programs, Avast or Avira if you want a free one.

- b. Use the Windows Firewall built into XP, Vista, and Windows 7.
- c. Install the free version of MalwareBytes' Anti-Malware (MBAM) from <http://www.malwarebytes.org>. Update it and do a Quick Scan once a week. Vista and Windows 7 have Windows Defender built into them. I don't care for WD in XP and I don't like antispyware programs that run resident in the background, but it doesn't hurt to have WD in Vista/Win7. There is no need to have more than these antispyware programs installed.
- d. Keep Windows patched. Keep major programs that are known vectors for attacks updated - Microsoft Office, Adobe Reader, Java, Adobe Flash Player.
- e. Do other general maintenance regularly. See - <http://www.elephantboycomputers.com/page2.html#Maintenance> for more details.
- f. And remember to practice safe computing. None of the foregoing will help you if you indulge in risky behavior. See #4, "Practice Safe Hex" here – http://www.elephantboycomputers.com/page2.html#Removing_Malware (scroll down to "E. After the machine is clean").