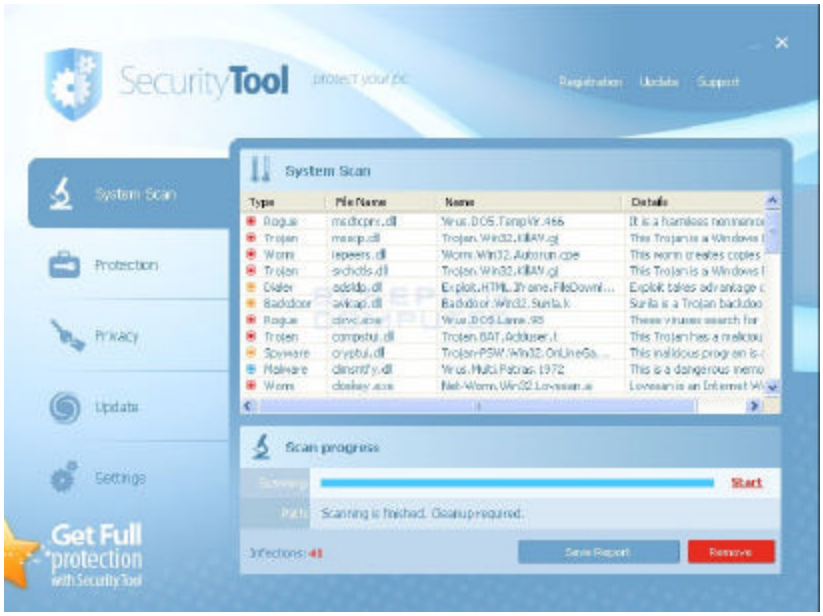
# Fake Security Software Warning

## Compiled by John Nozum
## Owner of Knoz'em Computers, LLC

Since around the year 2008, there has been an explosion of fake "security" software. Going to bad sites, such as many porn sites, illegal video downloading sites, and illegal music downloading sites is just ASKING for trouble. However, you do not necessarily have to go to a bad site in order to get "nailed". Sometimes, ad servers can be infected, and you don't have much control over this. Fortunately newer virus checkers are trying to catch up with the latest slime balls out there. Anyway, you may be browsing on line, and all in sudden, you get a pop-up saying that your system is infected and/or X number of Trojans have been found. You may be given the "option" to "fix" these problems. DO NOT FALL FOR THIS!!! THIS IS A WOLF IN SHEEP CLOTHING!!! If you see a pop-up saying that your system in infected, LOOK CLOSELY to see if you see the logo and/or name for YOUR virus checker (i.e. AVG, Norton, or whatever). If you do not see this, it is more cause for alarm. Below are a couple of screen shots of illegitimate "security" software.

Here is another fake “security” program.




If one of these boogers comes up on the screen, do NOT click on “No” or even the red ‘X” if there is one. Under the hood, it is “YES” and “YES”—I want to be infected!!! Instead, here is what to do:

If your system was built after about 2002 or 2003, you can try the simpler method IF you have nothing that needs to be saved:

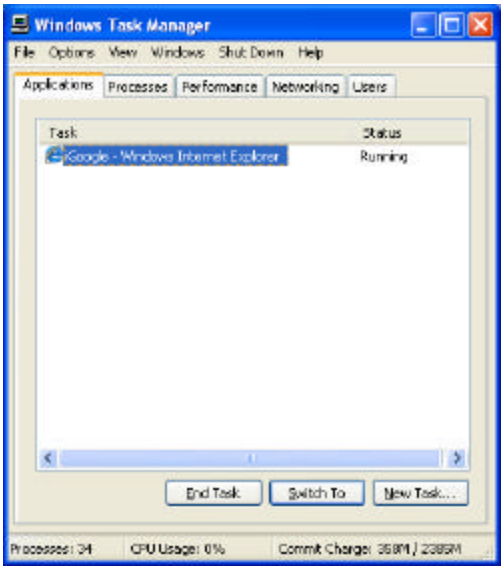
1. Push in on the power button for 1 second or less. This should force the system through a “normal” shutdown. If you get warnings about programs not wanting to close, tell them to “End now”.
2. Wait a few seconds and then restart the system normally.

If the above fails, you may need to do an EMERGEN CY shutdown. Holding in on the power button for about 5 seconds will invoke the emergency shutdown.

Now if you have other stuff that needs to be saved, you can try to terminate Internet Explorer (and its attached virus or whatever) or other browser by doing the following:

1. Hit CTRL-ALT-DEL (all at the same time)

2. Go the Applications tab.




3. Look for an entry that pertains to the suspicious "security" program. Often there will be none. If that is the case, then kill the browser (i.e. Internet Explorer, Firefox, Netscape, Opera, AOL, or whatever). Single click on this, and then click on "End Task" toward the bottom of this window.
4. At this point, it should kill Internet Explorer or whatever—along with the threatening "security" warning.
5. Do a normal reboot (restart). You want to break any ties with these slime balls!

**UNDER NO CIRCUMSTANCES** should you ever buy the "full version" to "fix" your problem! This is the pinnacle of it all—They want your credit card number!!! Worse yet, it may be VERY DIFFICULT to get your money back! This is often called "smitfraud". I have heard where even if you do buy the "full version", your computer is NOT fixed, but still left infected. In addition, many fake "security" programs will DISABLE your real security software! If you ever get to where you can not update your real security software, but you can do other things, there is probably malware already in your computer.

For the slime balls that write this crap, here is a WONDERFUL place for them:

A cell at the old West Virginia State
Penitentiary in Moundsville, WV

May God's peace be with you, but may these slime balls
be brought to justice!

***John G. Nozum***
***Owner of Knoz'em Computers, LLC***

***Last updated on January 24, 2011***