Are you scared enough of scareware?

Litigation began in King County Superior Court against Texas defendants alleged to have sent electronic messages to people in Washington state consisting of what appeared to be an error-message box with the words CRITICAL ERROR MESSAGE! REGISTRY DAMAGED AND CORRUPTED.
The message box directs the user to a web site where a scan of the user's computer is offered. The scan shows a number of alleged registry errors and the user-victim is offered software (for a fee) to fix the errors.
See State of Washington v. McCreary et. al./, King County Cause # 08-2-33486-4. (Complaint available online at http://atg.wa.gov/uploadedfiles/Home/Press_Releases/2008/ComplaintRegistryCleaner.pdf.) The lawsuit was brought under Washington's new Computer Spyware Act (RCW 19.270) and the Unfair Business Practices Consumer Protection Act (RCW 19.86).

The registry is a critical part of a computer's operating system where many settings relevant to day-to-day computer use are set and monitored. Damage or corruption to the registry is scary for many computer users because mastering the registry is very complex and not a tool the average computer user opens and studies every day. That is why the messages in this case are referred to as scareware, a problem that has become pervasive enough to generate comments on weblogs and mail lists around the world.

What makes this problem worse is that most Internet users cannot distinguish between genuine warnings and false messages that can spread viruses and other malware. A study published September 22, 2008, in the "Proceedings of the Human Factors and Ergonomics Society" presented the results of North Carolina State University research on how willing participants were to open suspicious files when warned. Participants could not discern the (subtle) differences between real error messages and fake ones. Sixty-three percent of the time they opened the fake messages, exposing their computers to malware and themselves to frustration and expense.

One approach to scareware is not to be intimidated and to ignore it. But there will always be a bit of suspicion and second-guessing that is caused by the emotional nature of the warning, our own lack of knowledge of the nature of the threat, and our unwillingness to admit ignorance of the issues and complexities the threat poses. So a more practical approach to the problem of scareware dissolves the emotion. First go to the web site of the operating system creator. That would be Microsoft http://www.microsoft.com, Apple http://www.apple.com, or the web site of the creator of the Linux distribution you are using. Once there, search for a list of error codes. When you find that list, check the error code number for the relevant message. That message will tell you what is wrong and what to do about it. If the error code in the message is not in the list of error codes you retrieve, the message is probably bogus.

Once you find out what is wrong, go to the Sans Institute web site at http://www.sans.org and find out what you can about the registry error. The good news is that you will not need to know much because your next step will solve the problem.

The third and final step is to go to a credible web site such as http://www.download.com and search for registry repair software. Notice that this is a search initiated by you on a site chosen by you as opposed to an emotion-fueled direction to a particular web site chosen by someone else. Search for registry repair and several tools will be offered to you. These have been vetted and will be spyware- and malware-free. Pick one, download it, prepare it, then run it. Chances are you will not have a problem. By your own action, you will have dissolved the scare of scareware.