

**Computer Troubleshooters
Kanata**

Info@ctkanata.com
http://www.ctkanata.com

T: 613.864.0820
F: 613.271.1231

Offices Worldwide

Australia, Austria, Bahrain,
Bulgaria, Botswana, Canada,
Colombia, Democratic
Republic of the Congo, Egypt,
Ethiopia, Ghana, Greece,
Guatemala, Hong Kong,
India, Kenya, Kuwait,
Malaysia, Mexico,
Netherlands, New Zealand,
Nigeria, Portugal, Republic of
Ireland, Romania, Singapore,
South Africa, Spain, United
Kingdom, United States of
America

International Website

www.comptroub.com

Computer Troubleshooters
The World's #1 computer
service franchise network



OVER
450
LOCATIONS WORLDWIDE


For Immediate release

Blackhat SEO

One of the most frequent threat methods on the Internet today is Blackhat SEO. Blackhat SEO is a criminally motivated **S**earch **E**ngine **O**ptimization technique. This technique allows cyber-criminals to promote malware campaigns based on top search results linked up to the most relevant/recent news topics. These attacks are often automated, as the cyber-criminals are able to leverage Google trends to figure out what are the most relevant/recent news.

Enter fake antivirus programs. These applications pass themselves off as antivirus products, and claim to detect hundreds of threats on your computer. When you try to remove the threats with the application, you are then asked to purchase a corresponding license. You are naturally worried about the supposed infection, will often buy the license. Once you have handed over your money, you will no longer hear from the 'vendors' and the fake antivirus will remain on your computer.

These applications have been in circulation for several years, but it wasn't until early 2008 that cyber-criminals adopted fake antivirus on a massive scale.

Many fake antivirus programs share a number of commonalities:

- They display fake pop-up warnings, launch messages in the task bar and make changes to the screensaver and desktop
- Their design is similar to that of a real antivirus product
- They complete scanning of the entire system very quickly
- The 'infections' detected often refer to different files on each scan

Fake antivirus programs also make a series of alterations to the operating system in order to prevent their fake warnings from being removed. This includes hiding the Desktop and Screensaver tabs from the Display properties section. This way, you cannot restore the desktop theme or the screensaver. The purpose of these techniques is to exhaust the your patience so that they finally register the product and pay the corresponding fee.

[PandaLabs](#), [Panda Security's](#) anti malware laboratory, has recently detected the proliferation in search engines of numerous Web pages distributing the [MySecurityEngine](#) fake antivirus. The 'bait' used in this case has been the much anticipated final episode of the popular ABC series "Lost." According to Luis Corrons, Technical Director of [PandaLabs](#), "What continues to surprise us is the speed with which the numerous websites are created and then indexed and positioned on the Internet. As the screening of the final episode of "Lost" approaches we expect the number of malicious links to double or triple."

Be wary when visiting websites through search engines, and try to make sure the pages you visit are reliable. If users should be directed to fake websites, it is essential that no downloads are accepted. "Using your common sense and having good up-to-date protection installed are the two best ways of staying safe from these threats.



Contact your local Computer
Troubleshooters

Norman Schweitzer
613.864.0820