Security
April 27, 2009 9:01 PM PDT

McAfee launches free online cybercrime help center

by Elinor Mills

Is your computer acting funny? Are you worried that you may have visited a malicious Web site or opened an e-mail attachment with malware?

Instead of worrying about it you can now go to a new Web site McAfee is launching on Tuesday that is designed to help computer users figure out if they have legitimate reason to be concerned.

The new **Cybercrime Response Unit** offers a forensic scanning tool that checks for malware on the computer and cookies left by suspicious Web sites to help determine if the machine has been compromised. A toll-free number is available for people whose scan results are worrisome.

I gave it a test run and decided to have my mother try it out too. The home page is full of information and links related to McAfee's cybercrime strategy and it's not immediately clear where to go. There is a link to "Cybercrime Response Unit" at the top, along with other links and at the bottom, but if you don't know the name of the help center it wouldn't be readily apparent that that is what you are looking for. It would be nice to have a special box prominently placed that says something like "To find out if your machine is at risk, click here."

The prompts thereafter are straightforward. The main Cybercrime Response Unit page explains that the site will help determine the likelihood that the computer or a user's habits may be linked to fraudulent activities, guide victims to the financial institutions and creditors to clear up any fraudulent activity, and report any crime to law enforcement. There's also a five-minute video explaining what the site is about.

If visitors feel they may have been victimized by cybercrime, they can click through to a page that contains a series of questions that will be used to determine the level of risk. They are asked whether there are unexplained charges or suspicious activity on any financial accounts or other indications of identity fraud and whether the computer is running more slowly than usual, displaying pop ads, or having difficulty shutting down or starting up.

There are also questions about user behavior, including whether the visitor responded to an e-mail or Web site request for personal information that may have been a scam, whether an e-mail attachment was opened that could have been malicious, and whether the computer was lost or stolen.

The visitor is then prompted to run the McAfee Cybercrime Scanner. However, the tool does not run on **Firefox** so my mother and I both had to open Internet Explorer and start the process over. (McAfee says the Firefox version is coming but could not provide a time frame.) The scanner looks for unwanted processes or unauthorized programs running on the computer, visits to known malicious Web sites, unauthorized connections to the computer, unauthorized modifications to the computer protections, security sessions or browser and other unauthorized activity.

Results from my scan revealed that I had cookies on my system from visiting a malicious Web site. (Credit: McAfee)

It took less than five minutes to scan my mother's home PC and close to 15 minutes to scan my office PC. The outcomes were similar. My machine was found to have cookies from one suspicious domain, which it listed and recognized as high risk. I did not recognize the site and couldn't find it in Google either. My mother's machine had cookies from two other suspicious domains, one of which was deemed high risk and the other medium risk.

The site said we were both at high risk of being victims of cybercrime or fraud and recommended that we place fraud alerts with credit reporting agencies and report signs

of potential fraud. It also suggested that we install **McAfee's SiteAdvisor**, a free antiphishing toolbar.

That is all good advice, although I wasn't ready to place a fraud alert based just on the fact that I had visited one potentially malicious site when my machine is loaded with up-to-date antivirus and other security software.

"Many of these sites that trigger red flags host malicious software and you could have downloaded a keylogger or other malicious software on the PC," McAfee cybercrime strategist Pamela Warren said in an interview.

"If you have the latest virus definitions, 9 times out of 10 you're going to be safe," she said. "I'd rather be proactive in terms of seeking a fraud alert now versus rebuilding six month of my life and getting my credit history back in check."

I called the toll-free number to see what they would say. A gentleman with a Spanish name but speaking excellent English answered and asked for my session ID so he could see the results of my scan. Then he explained that I may have been exposed to a malicious Web site from surfing. He said the results don't mean my machine is infected or has been compromised, but said I should use SiteAdvisor to help protect the computer from malicious sites in the future.

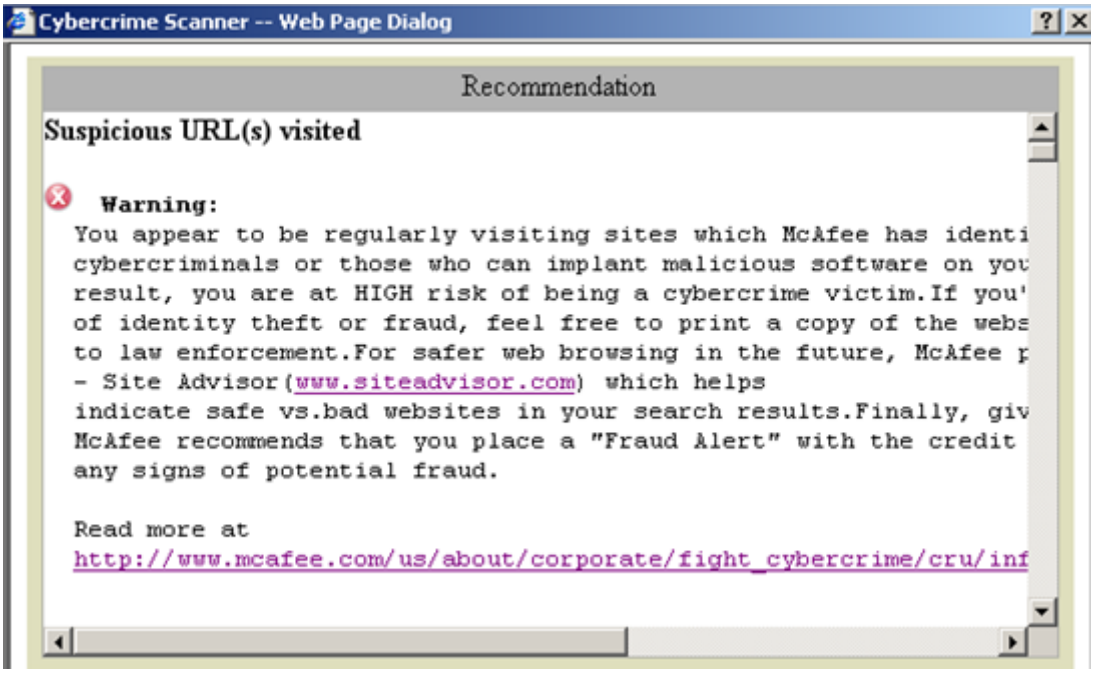
Neither my mother nor I were alarmed but I urged her to go ahead and install SiteAdvisor and place a fraud alert, just in case.

Given how many people still get hit with worms and other malware and tricked into providing sensitive information on phishing site, it's clear that the best way to change this is through education. The McAfee Cybercrime Response Unit provides the electronic equivalent of hand holding for consumers as they try to figure out whether they have been victimized and what to do if they have been.

After using the site, my mother has a better handle on the different types of risky behavior. As for the site design, she said she liked the fact that there were no ads or blatant marketing on the site and that it had a lot of useful information, such as links to other resources and detailed steps to take to report financial fraud or a crime and tips on best practices for things like protecting your computer and using social networking

sites.

"If I had taken the time to read more (of the information on the site) I would have learned more," she said.



McAfee's Cybercrime Scanner makes recommendations based on a light scan of a computer.
(Credit: McAfee)

Elinor Mills covers Internet security and privacy. She joined CNET News in 2005 after working as a foreign correspondent for Reuters in Portugal and writing for The Industry Standard, the IDG News Service, and the Associated Press. E-mail Elinor.

Topics: **Vulnerabilities & attacks**

Tags: **McAfee Cybercrime Response Unit**

Share: Digg Del.icio.us Reddit Yahoo! Buzz Facebook

Related

From CNET

At Finovate, a bad economy means good start-ups

Puerto Rico sites redirected in DNS attack

KnowEm searches 120 sites for open user names

From around the web

McAfee, Inc. Offers Tips and Advice in R... AOL News

False Security: 'Scareware' Spreads Wall Street Journal

More related posts powered by Sphere