June 2012

Fraud Alert!

C.A.S.E. Program – From Weld County District Attorney Kenneth R. Buck

Check Your Computer for the "Internet Doomsday" Malware

Last year, a group of cyber criminals began distributing computer malware known as the "DNSChanger." Malware is a type of software that hackers and other criminals distribute to exploit your computer. The DNSChanger malware fools computers into sending users to fraudulent websites or to interfere with your Web browsing. About 350,000 computers are infected today.

On July 9, the FBI will shut down a temporary network of computer servers that are supporting people who have infected computers. If your computer is infected with the DNSChanger malware, that means the Internet may not work for you beginning July 9. Fortunately, there are steps you can take now to see whether your computer is infected and to remove the malware, if necessary.

Is My Computer Infected?

The best way to determine if your computer or router has been affected by DNSChanger is to have them evaluated by a computer professional. However, you can also perform a simple check by going online to **http://www.dns-ok.us/**

If your computer is not infected with the DNSChanger malware, the background on the screen will appear green. If your computer is infected, the background will appear red.

What If My Computer is Infected?:

If your computer is infected with the DNSChanger malware, it's best to have a computer professional evaluate and remove the malware for you. If you are comfortable with computer systems, you can also visit **www.dcwg.org** for information about how to remove the threat.

For additional information, or to report being a victim of the DNSChanger software, visit **www.fbi.gov**.

Immediately report to your local police agency if you think you are a victim of crime.
To view other Fraud Alerts, go to www.weldda.com.