FROM WELD COUNTY DISTRICT ATTORNEY KENNETH R. BUCK
FOR THE C.A.S.E. PROGRAM

FRAUD ALERT!

DON'T TAKE THE BAIT

Internet crime complaints continue to rise according to the Internet Crime Complaint Center (iC3.gov) which recently reported that it received 336,655 complaints in 2009 (up 22% from 2008 and up 45% from 2005). Their press release went on to state that in 2009 internet crimes resulted in approximately $559.7 million in loss to the victims.

Are you the type of person who reads a fraud alert or news story and asks yourself, "Who actually falls for these internet phishing scams?" Consumer Reports reported in June of 2009 that approximately 1 in 90 people do. That is a fairly good rate of return for fraudsters who send out thousands of phishing emails daily.

Phishing, a play on the word fishing, is a legitimate looking — but fraudulent — email that "baits" the victim with false information (you have won the lottery; receive a $25 gift card to a national-chain store for filling out this survey; there is problem with your bank account or store order) and then sets out the "hook" to catch the victim. The "hook" is usually a link in the email that takes you to a web site where you are asked to enter personal financial information such as bank account numbers, Social Security numbers, credit or debit account numbers, etc. Once you do that, you have provided the con artist with the information they need to access your finances.

The first rule for not falling victim to a phishing scam: don't respond to unsolicited emails. If you think an email might be legitimate, do not follow the embedded links (again, especially not in unsolicited emails). It used to be that you could verify a secure web site by checking the URL (web page address) and see the "http" change to "https". You could also look for the locked pad lock icon on the web page. Phishers, however, are now able to forge both web address and the locked pad lock icon. That being said, individuals need to be even more diligent about making sure they are dealing with a legitimate company on a truly secure site. Type the URL of your bank, credit card issuer, retail site, etc., directly into your browser. Click on the pad lock icon of that page and verify its security certificate — if it is not a legitimate site you should get warnings about the certificate after you click on it. Also, consider using web browser tools that alert you to known fraudulent web sites. Internet Explorer 7, Firefox version 2 and EarthLink Scamblocker are all examples of browsers that offer such a tool bar.