FRAUD ALERT!

Don't be a Victim of Phishing

Many Internet users are receiving E-mails requesting personal and confidential account information. The e-mail sender often poses as a bank, government agency, or companies like eBay and PayPal. In reality the sender is a criminal.

Attempts to steal your sensitive information are called "phishing," a scheme that has become very prevalent. The sender goes "phishing" for your information usually by setting up a phony website at which you are asked to supply information - account numbers, passwords, pin numbers, Social Security Numbers. If you provide that information, your accounts and other assets may be stolen.

To protect yourself, simply do not open or respond to e-mails asking to submit personal information. The message might include fancy graphics, trademark symbols and an authentic-looking e-mail address, but all of that can be faked. Here are some ways to tell:

- ✓ The message tries to scare or upset you by saying your account needs to be verified or updated.
- ✓ The message threatens negative action, such as canceling your account, if you fail to take the requested action immediately.
- ✓ The message asks you to click on a link to update or submit your information. Legitimate e-mails will not contain a link, but will ask you to close out the message, open the company's Internet Web site, and use your name and password to update the required information. Never click on a link!
- ✓ The message is addressed to "Dear Customer" instead of your name.

JEFF W. REISIG
YOLO COUNTY DISTRICT ATTORNEY
ELDER PROTECTION UNIT
(530) 666-8416