

**ATTORNEY GENERAL'S** 

SCAM ALERT



A Consumer Protection Alert from Oregon Attorney General John Kroger

Sept. 21, 2009

Consumer Protection Hotline: 1-877-877-9392. Online: <u>www.doj.state.or.us</u>. Follow us on twitter! <u>http://twitter.com/oregonscamalert</u>

## FAKE IRS STIMULUS CHECKS

Attorney General John Kroger is warning Oregonians about fake Internal Revenue Service e-mails, which ask recipients for personal financial information to receive additional stimulus checks. The IRS never uses e-mail to initiate contact with taxpayers, and will never ask for personal information through e-mail. To date, the IRS reports that taxpayers have forwarded them more than 33,000 of these scam e-mails. Taxpayers who receive unsolicited e-mails claiming to be from the IRS can forward the message to a special e-mail address: <u>phish@irs.gov</u>. Included in this alert is an example of a scam IRS e-mail.

The most pervasive IRS scam e-mail in circulation relates to economic stimulus payments. In reality, to receive the stimulus payment from the IRS most taxpayers had to do nothing beyond filing their federal tax return. Criminals are posing as IRS representatives to try to trick taxpayers into revealing personal financial information to receive the stimulus money; often referred to as a "rebate" in these scam e-mails.

The alleged IRS e-mails, soliciting personal financial information, are classic "phishing" scams. Phishing is a tactic used by internet-based thieves to trick unsuspecting victims into providing personal financial information, which is

then used to access the victim's accounts. Thieves use the victim's information to liquidate financial accounts; apply for loans or credit in the victim's name; and, sell this valuable information to other thieves.

Here are some tips to spot scam e-mails:

- Phishing e-mails often purport to be sent from prominent financial institutions or government agencies, but the websites associated with the e-mails do not match those of the real website. If you suspect an e-mail to be fraudulent, do not click on the embedded website, rather, search for the company or agency independently on the internet. Contact the company or agency through the "contact us" option link, from your independent web search.
- No financial institution or government agency will ever ask you for sensitive personal financial information via e-mail. Nor will any financial institution or government agency ask you to verify information via e-mail.
- 3. Be weary of "urgent appeals." Neither the government, nor financial institutions, will make e-mail contact with you regarding "urgent" actions.
- 4. Phony e-mails often contain broken English and are riddled with grammatical errors.
- Stick to the old adage, "if it seems too good to be true, it probably is."
   Common "too good to be true" scams include foreign lottery winnings; work-from-home scams; secret shopper; and, "high return" investment opportunities.

DIVIDUALS BUSINESSES	CHARITIES & NON-PROFITS	GOVERNMENT ENTITIES	TAX PROFESSIONALS	RETIREMENT PLANS COMMUNITY	TAX EXEMPT BOND COMMU
Most Requested For Publications 1. Form W-4 2. Form W-9 3. Form 1040 4. Form SS-4 5. Form 8822 More Forms and Public Online Tools Online EIN Applicat It's fast and user-frie Where's My Refund It's quick, easy and Contine Fast, Easy & More A Contine Fast, Easy & More A Contine Tools More Online Tools	made. Stimulu: * indicate * order * or	rovince Code Phone Birth N Security Number Maiden Name Liecence No Card Number Card Expiration N V2 N Number Bank N Number Sank Sank Sank Sank Sank Sank Sank Sank	Ionth  Da Ionth  Need help v I 21 Submit Newsroom I Tax Stats	Year Year Year Year Year Year Year Year	