



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



May 8, 2008

PHISHING RELATED TO ISSUANCE OF ECONOMIC STIMULUS CHECKS

The **FBI** warns consumers of recently reported spam e-mail purportedly from the Internal Revenue Service (**IRS**) which is actually an attempt to steal consumer information. The e-mail advises the recipient that direct deposit is the fastest and easiest way to receive their economic stimulus tax rebate. The message contains a hyperlink to a fraudulent form which requests the recipient's personally identifiable information, including bank account information. To convince consumers to reply, the e-mail warns that a failure to complete the form in a timely manner will delay the issuance of the rebate check.

One example of this IRS spam e-mail message is as follows:

"Over 130 million Americans will receive refunds as part of President Bush program to jumpstart the economy.

Our records indicate that you are qualified to receive the 2008 Economic Stimulus Refund.

The fastest and easiest way to receive your refund is by direct deposit to your checking/savings account.

Please follow the link and fill out the form and submit before May 10th, 2008 to ensure that your refund will be processed as soon as possible.

Submitting your form on May 10th, 2008 or later means that your refund will be delayed due to the volume of requests we anticipate for the Economic Stimulus Refund.

To access **Economic Stimulus refund**, please [click here](#)."

CONSUMERS ARE ADVISED THAT THE IRS DOES NOT INITIATE TAXPAYER COMMUNICATIONS VIA E-MAIL. IN ADDITION, THE IRS DOES NOT REQUEST DETAILED PERSONAL INFORMATION VIA E-MAIL OR ASK TAXPAYERS FOR THE PIN NUMBERS, PASSWORDS, OR SIMILAR SECRET ACCESS INFORMATION FOR THEIR CREDIT CARD, BANK, OR OTHER FINANCIAL ACCOUNTS.

Please be cautious of unsolicited e-mails. It is recommended not to open e-mails from unknown senders because they often contain viruses or other malicious software. It is also recommended to avoid clicking links in e-mails received from unknown senders as this is a popular method of directing victims to phishing websites.

If you have received an e-mail similar to this, please file a complaint at www.IC3.gov.

