

Consumer Affairs Agencies

Division of Banks

Division of Insurance

Division of Professional Licensure

*Department of
Telecommunications and Cable*

Division of Standards

State Racing Commission

Massachusetts Office of Consumer Affairs & Business Regulation

CONSUMER ADVISORY

IRS Phishing Scam: Tax Refund E-mail

The Office of Consumer Affairs and Business Regulation wants consumers to be aware of e-mail messages claiming to be from the Internal Revenue Service (IRS). Scammers are fraudulently using the IRS name and/or logo to gain access to consumers' financial information.

"Phishing" is a type of deception designed to steal your valuable personal information, such as credit card numbers, passwords, account data, or other information. Scammers send millions of fraudulent e-mail messages that appear to come from web sites you trust, like the IRS, your bank, or your credit card company, and request that you provide personal information.

A most recent phishing scam uses an e-mail claiming to be from the IRS telling recipients that they are due a tax refund, which can be received by clicking on a link in the e-mail. The subject line of the e-mail message says: "Tax Refund: \$252.60" (or some other dollar amount).

Please be advised that the IRS does not send unsolicited e-mail messages, warnings, or requests for your information, so unless you are actively working with someone at the IRS, you should assume that anything claiming to be from the IRS is not valid.

"Don't let someone take advantage you," said Daniel Crane, Undersecretary of the Office of Consumer Affairs and Business Regulation. "Be wary of e-mails asking for your personal information. To see if the e-mail is legitimate, close out of your e-mail and log onto the purported sender's site directly."

To prevent phishing, e-mail scams, and bogus IRS Web sites, the IRS offers the following tips:

1. Do not reply to suspicious e-mail messages.
2. Do not open any attachments or links, as they may contain a malicious code that will infect your computer.
3. Forward the e-mail or Web site URL to the IRS at phishing@irs.gov.
4. After you forward the e-mail or Web site URL to the IRS, delete the e-mail message from your computer.

For more information on phishing scams that use the IRS, click on the following link: [IRS Phishing Scams](#).

Daniel C. Crane
Undersecretary

10 Park Plaza
Suite 5170
Boston, MA 02116

Hotline:
617-973-3787
888-283-3757

www.mass.gov/consumer