

## IRS Name Used in Phony E-mail and Telephone Scams

May 12, 2008

### Summary

The IRS has reported that their name and logo are being used fraudulently to lure taxpayers into divulging their financial information.

State(s): All States

Type of Alert: E-mail and Telephone Scams

### [Loss Prevention Recommendations](#)



CUNA Mutual alerts credit unions of this risk. Please pass this information on to all appropriate employees. If your credit union has experienced a loss, contact our Credit Union Protection Response Center at 1-800-637-2676.

### Details:

The Internal Revenue Service has issued an alert, warning that the IRS name and logo is being used by fraudsters attempting to access the taxpayer financial information through e-mail, telephone, and cell phone text messaging.

**Note: The IRS does not ask for personal identifying or financial information via unsolicited e-mail, telephone calls, or text messaging.**

The following scams are being used to trick taxpayers into divulging financial account information for fraudulent purposes:

- Taxpayers receive a phone calls telling them that they are eligible for a sizable rebate for filing their taxes early, and they are told to provide their financial account information for direct deposit.
- Taxpayers receive e-mails that claim they are eligible for a tax refund of a specific amount, and they are instructed to click on the link in the e-mail to access the refund claim form, which requires them to disclose financial account information.
- E-mail notifications addressed to individual taxpayers claim that their tax returns will be audited. The individual is instructed to click on the link within the e-mail and complete forms disclosing personal and financial account information.
- Businesses, accountants, and "Treasury" managers are receiving bogus e-mails regarding tax law changes. To obtain information on publications for businesses, estates taxes, excise taxes, exempt organizations, as well as IRAs and other retirement plans, the recipient is instructed to click on a series of links. The IRS

suspects that clicking on these links downloads “malware” onto the recipient’s computer, which can be used to search for financial records and other private information.

- A person claiming to be an IRS employee telephones taxpayers to say the IRS has mailed them a check that has not been cashed. The caller then asks for verification of financial account information.

### **Loss Prevention Recommendations:**

If you receive an unsolicited e-mail purporting to be from the IRS, take the following steps:

- Do not open any attachments to the e-mail; they could contain malicious code that will infect your computer.
- Forward a questionable e-mail claiming to be from the IRS to [phishing@irs.gov](mailto:phishing@irs.gov).
- Use instructions contained in an article online at [www.irs.gov](http://www.irs.gov) titled “[How to Protect Yourself from Suspicious E-Mails or Phishing Schemes.](#)”
- Contact the IRS at 800-829-1040 to determine whether the IRS is trying to contact you about a tax refund.
- Remember that taxpayers do not have to complete a special form to obtain a refund.
- If you have received this, or a similar hoax, please file a complaint at [www.ic3.gov](http://www.ic3.gov).
- Educate your membership on “Phishing.”
  - Post “phishing warnings” on your Web site, in newsletters and in your lobby.
  - Post a notice on your credit union's Web site that you will never solicit personal or private information via e-mail.
  - Use the [Federal Trade Commission Web site](#).
    - Consumers can take interactive quizzes designed to enlighten them about identity theft, phishing, spam and online-shopping scams.
    - Elsewhere on the site, consumers can find detailed guidance on how to monitor their credit histories, use effective passwords and recover from identity theft.
- If a member is a victim of a "phishing email," take appropriate steps to help protect him/her.
  - Block and reissue the compromised credit/debit cards.
  - Report to credit bureau.
  - Order credit report.
- A good resource for this topic is [Anti-Phishing Working Group](#).
- If you have been the victim of a spoof e-mail or Web site, you should contact your local law enforcement, a U.S. Postal Inspector, or the FBI.

If you are aware of a risk in your area, whether it has struck your credit union or not, please complete the [Report a RISK Alert](#) form.

The information contained in this RISK Alert is intended for the sole use of our Credit Union Bond policyholders to prevent fraud losses. Any further distribution of this information could subject you to liability under common law and various statutes including the Fair Credit Reporting Act.

CUNA Mutual Group does not provide any warranties or guarantees with respect to the performance of services by any vendor, and is not liable for any products or services purchased from any vendor by any credit union. Each credit union is ultimately responsible for determining the products and services that it may require, selecting the vendor that best meets the credit union's needs (whether or not a preferred partner), and contracting directly with that vendor.