CTSI
Serving Colorado's Counties

Technical Update

Volume 13, Number 27 September 29, 2009

Email Scam Alert

In keeping with the mission statement of CTSI, we want to provide you with technical services that are progressive and cutting edge loss prevention. A recent Internal Revenue Service warning has prompted us to inform our members of recent identity theft scams that can be harmful to our county members. These scams have used the IRS name, logo or website in an attempt to convince taxpayers that they are receiving a genuine communication from the IRS. Scammers may use other federal agency names, such as the U.S. Department of the Treasury.

The scams may take place through email (phishing), fax or phone. The IRS does not discuss tax account matters with taxpayers by email. Knowing this could mean the difference between keeping your identity intact and falling prey to identity thieves.

The Scam-Making Work Pay

This phishing email, which claims to come from the IRS, references the president and the Making Work Pay provision of the 2009 economic recovery law. It says that there is a refundable credit available to workers, consumers and retirees that can be paid into the recipient's bank account if the recipient registers their account information with the IRS. The email contains links to register the account and to claim the tax refund.

The Reality- Making Work Pay

Most taxpayers receive their Making Work Pay refund through their paycheck as a credit toward their tax withholding, not as a lump sum distribution. Additionally, consumers and retirees who are not wage earners are not eligible for this tax credit.

The Scam-Tax Refund Link

This bogus email, which claims to come from the IRS, tells the recipient that he or she is eligible to receive a tax refund for a given amount. It instructs the recipient to click on a link contained in the email to access and complete a form for the tax refund. The form requires the entry of personal and financial information. The Tax Refund Scam is the most common one seen by the IRS. Recent scam variations have claimed to come from the Exempt Organizations area of the IRS. Others include the name and purported signature of a genuine or a made-up IRS executive.

The Reality-Tax Refund Link

Taxpayers do not have to complete a special form to obtain a refund. Taxpayer refunds are based on the tax return they submit to the IRS.

The Scamp-Inherited Funds / Lottery Winnings / Cash Consignment

In this phishing scheme, recipients receive an email claiming to come from the U.S. Department of the Treasury notifying them that they will receive millions of dollars in recovered funds or lottery winnings or cash consignment if they provide certain personal and financial information via return email.

In some scams, a person may be sent a phony check of the funds or winnings and told to deposit it but to return 10 percent in taxes or fees. Thinking that the check must have cleared the bank and is genuine, some people comply. However, the scammers, not the Treasury Department, will get the taxes or fees.

800 Grant St., Suite 400
Denver CO 80203

County Technical Services, Inc.

303.861.0507
FAX: 303.861.2832

CTSI
Serving Colorado's Counties

Technical Update

Volume 13, Number 27 September 29, 2009

Email Scam Alert - Part 2

How to Spot a Scam

Many email scams are fairly sophisticated and hard to detect. However, there are signs to watch for.

- The email requests detailed or an unusual amount of personal and/or financial information, such as name, SSN, bank or credit card account numbers or security-related information, such as mother's maiden name. The request may be in the email itself or on another site to which a link in the email sends the recipient.
- The email dangles bait to get the recipient to respond to the email, such as mentioning a tax refund or offering to pay the recipient to participate in an IRS survey.
- The email threatens a consequence for not responding to the email, such as additional taxes or blocking access to the recipient's funds.
- The email spells the Internal Revenue Service or other federal agency names wrong.
- The email uses incorrect grammar or odd phrasing (many of the email scams originate overseas and are written by non-native English speakers).
- The email uses a really long address in any link contained in the email message or one that does not start with the actual IRS Web site address, www.irs.gov.

What This Means For Counties

The IRS does not initiate taxpayer contact via unsolicited email or ask for personal identifying or financial information via email. If you receive a suspicious email claiming to come from the IRS, take the following steps:

- Do not open any attachments to the email
- Do not click on any links, in the email
- Contact the IRS at 1-800-829-1040 to determine whether the IRS is trying to contact you.
- Forward the suspicious email to the IRS mailbox, phishing@irs.gov, then delete the email from your inbox.

The only genuine IRS website is www.irs.gov. All irs.gov web page addresses begin with http://www.irs.gov/. Anyone wishing to access the IRS website should initiate contact by typing www.irs.gov into the internet address window rather than clicking on a link in an email.

800 Grant St., Suite 400
Denver CO 80203

County Technical Services, Inc.

303.861.0507
FAX: 303.861.2832