COMPTROLLER of MARYLAND
Serving the People

Peter Franchot

TAXPAYER *Tips*

IRS: Don't Fall for Scam Calls and Emails

ANNAPOLIS, MD (February 7, 2017) -- Scams continue to use the IRS as a lure. These tax scams take many different forms. The most common scams are phone calls and emails from thieves who pretend to be from the IRS. Scammers use the IRS name, logo or a fake website to try and steal money from taxpayers. Identity theft can also happen with these scams.

Taxpayers need to be wary of phone calls or automated messages from someone who claims to be from the IRS. Often these criminals will say the taxpayer owes money. They also demand payment right away. Other times scammers will lie to a taxpayer and say they are due a refund. The thieves ask for bank account information over the phone. The IRS warns taxpayers not to fall for these scams.

Below are several tips that will help filers avoid becoming a scam victim.

IRS employees will **NOT**:

- Call demanding immediate payment. The IRS will not call a taxpayer if they owe tax without first sending a bill in the mail.
- Demand payment without allowing the taxpayer to question or appeal the amount owed.
- Require the taxpayer pay their taxes a certain way. For example, demand taxpayers use a prepaid debit card.
- Ask for credit or debit card numbers over the phone.
- Threaten to contact local police or similar agencies to arrest the taxpayer for non-payment of taxes.
- Threaten legal action such as a lawsuit.

If a taxpayer doesn't owe or think they owe any tax, they should:

- Contact the Treasury Inspector General for Tax Administration. Use TIGTA's "IRS Impersonation Scam Reporting" web page to report the incident.
- Report the incident to the Federal Trade Commission. Use the "FTC Complaint Assistant" on FTC.gov. Please add "IRS Telephone Scam" to the comments of your report.

In most cases, an IRS phishing scam is an unsolicited, bogus email that claims to come from the IRS. Criminals often use fake refunds, phony tax bills or threats of an audit. Some emails link to sham websites that look real. The scammers' goal is to lure victims to give up their personal and financial information. If they get what they're after, they use it to steal a victim's money and their identity.

For those taxpayers who get a 'phishing' email, the IRS offers this advice:

- Don't reply to the message.
- Don't give out your personal or financial information.
- Forward the email to phishing@irs.gov. Then delete it.
- Do not open any attachments or click on any links. They may have malicious code that will infect your computer.

More information on how to report phishing or phone scams is available on IRS.gov.

###