Tax Scams

IRS warns of brazen tactics

By Cindy Hockenberry, EA

Following the emergence of more aggressive and widespread tax scams, the IRS issued another warning to taxpayers to remain on high alert and protect themselves against the deceitful tactics that scammers use to trick people.

In the latest variation, scammers alter what appears on your telephone caller ID to make it seem like they are with the IRS or another government agency. They'll utilize easily accessible online resources to get your name, address and other details about your life and use fake names, titles and badge numbers to make their calls sound official. They even go so far as to copy official IRS letterhead for use in email or postal mail. The objective remains the same—to trick taxpayers into providing personal financial information by scaring them into making a false tax payment that goes directly to the criminal.

Scammers posing as IRS agents first targeted those they viewed as most vulnerable, such as older Americans, newly arrived immigrants and those whose first language is not English. These criminals have expanded their net and will now target anyone. Chances are good that you or someone you know was a recipient of one of these aggressive phone calls.

Brazen scammers have even been known to provide their victims with directions to the nearest bank or business where the victim can obtain a means of payment, such as a debit card. In addition, con artists may then provide an actual IRS address where the victim can mail a receipt for the payment, all in an attempt to make the scheme look official. The most common theme with these tricks seems to be fear. Scammers try to scare people into reacting immediately without taking a moment to think through what is actually happening.

These scam artists often angrily threaten police arrest, deportation, license revocation or other similarly unpleasant things. They may also leave "urgent" callback requests, sometimes through "robo-calls," via phone or email. The emails will often contain a fake IRS document with a telephone number or email address for your reply.

It's important to remember that the official IRS website is IRS.gov. Don't be misled by sites claiming to be the IRS but ending in .com, .net, .org or other domains instead of .gov. Never provide personal information, financial or otherwise, to suspicious websites or strangers calling unexpectedly.

Scammers resort to tactics that the real IRS would never use. The IRS will never:

- Angrily demand immediate payment over the phone, nor will the agency call about taxes owed without first having mailed you a bill.
- Threaten to bring in local police or other law-enforcement groups to have you arrested for not paying.
- Demand that you pay taxes without giving you the opportunity to question or appeal the amount they say you owe.
- Require you to use a specific payment method for your taxes, such as a prepaid debit card.
- Ask for credit or debit card numbers over the phone.

Here's what you should do if you think you're the target of an IRS impersonation scam:

- If you actually do owe taxes, call the IRS at 800.829.1040. IRS workers can help you with a payment issue.
- If you know you don't owe taxes or don't believe you do, report the incident to the Treasury Inspector General for Tax Administration (TIGTA) at 800.366.4484.
- If you've been targeted by any scam, be sure to contact the Federal Trade Commission and use their FTC Compliant Assistant at FTC.gov. Please

add "IRS Telephone Scam" to the comments of your complaint.

TIGTA has received reports of roughly 600,000 contacts since October 2013. TIGTA is also aware of more than 4,000 victims who have collectively reported over $20 million in financial losses because of tax scams.

The IRS recently announced that the value of identity protection services is not taxable to individuals whose personal information was compromised in a data breach. Additionally, the IRS will not require that an employer who provides identity protection services to employees whose personal information was compromised in a data breach of the employer's recordkeeping system to include the value of the identity protection services in the employees' gross income and wages.

IR-2015-99, Ann. 2015-22