Financial Industry Regulatory Authority

Investor Alerts

Tools of the Fraud Trade: Phones and Emotions

The IRS impersonation scam is back, perfectly timed to coincide with the October 15 deadline for anyone who filed a federal tax extension last April.

The scam is a prime example of fraudsters using a very personal resource—your phone—as a weapon to try and take your money. It rings, and the person on the other end claims to be from the IRS. The caller is aggressive, sounds official, and demands immediate payment of taxes on the spot. Sometimes there are threats—pay up now, or face arrest or some other serious repercussion.

The scheme has certainly hit pay dirt. According to the Treasury Inspector General for Tax Administration, over 4,500 taxpayers have been victimized since October 2013, handing over some $23 million to the fraudsters.

FINRA's Securities Helpline for Seniors – HELPS™ has received a number of calls from investors, adding to the more than 700,000 people who have reported getting impersonation calls since the scam first surfaced in 2013. There are likely many more consumers who received a call or fell victim, who didn't report the scam.

Why Does the Scam Work?

When someone says they are from a government agency like the IRS, many of us may accept the statement as true. And in the case of the IRS impersonation scam, the reaction probably is accompanied by a surge of adrenaline. In the heat of the moment, hard-wired emotions can take over. You may not react with the typical caution you might use when you receive a call from a stranger.

Psychologists and behavioral economists have a name for the tactic these IRS impersonators use. It's called source credibility, and it's very powerful.

No Shortage of Tax Scams

From IRS impersonators to scammers claiming that you are about to be sued by the IRS and they can help, the list of tax and IRS-related scams is long and constantly changing. Learn more about Recent Tax Scams.

The fake tax collectors waste no time working to establish credibility. Impersonators use fake IRS badge numbers and caller ID numbers that are altered to look like they are from the IRS. In recent months, the impersonators have started to mail or fax official-looking “IRS” documents to people they have spoken with, hoping to trick them into sending money. Scammers may also try to trick you into providing personal information, which they can then use to file fake tax returns in your name to obtain and pocket a refund.

IRS impersonators use other tactics to build credibility. For instance, they might demand the name and contact information of your lawyer. The fake tax collectors know that you likely don't have an attorney, but their boldness in demanding this information makes them appear to be in a position of authority, which in turn adds to their credibility.

What Can You Do?

End a conversation with any unsolicited caller as quickly as possible. This severs the emotional hold the

fraudster has on potential victims. If you have caller ID, write down the number of the caller, if one appears. A blocked number is a sure sign of a fraud. And just because a number shows up doesn't mean it is real—it's likely a non-working number. The same logic applies to the name of the caller. Fraudsters have been known to illegally mimic or "spoof" the display so the call appears to originate from the IRS or another government agency.

Make no mistake about it, these calls are scams. Be skeptical of any unsolicited callers claiming to be from the IRS, and do not return the call if the scammer leaves you a voice message. As the IRS makes clear, it never calls taxpayers and demands that they wire or send money—instead the IRS sends a written notification of any tax due through the U.S. mail.

In addition, the real IRS **will not**:

- Demand that you pay taxes and not allow you to question or appeal the amount that you owe.
- Require that you pay your taxes a certain way, such as with a prepaid debit card.
- Ask for credit or debit card numbers over the phone.
- Threaten to bring in police or other agencies to arrest you for not paying.

After you hang up, if you feel the need to double check, call 1-800-366-4484 to determine if the caller is an IRS employee with a legitimate need to contact you. If the person calling you is an IRS employee, call them back. If not, report the incident to the IRS and to Treasury Inspector General along with the phone number that you may have retrieved during the call.

Visit FINRA's website for more tips on how to recognize and avoid financial fraud.

Last Updated: November 5, 2015
