

Is your personal info safe?

How to spot a tax scam



By Phillip R. McCollum, Jr., CPA, JD

When tax season rolls around, you aren't the only one eagerly awaiting your refund. Scammers are hoping to get their hands on your money first and there's no shortage of ways they're trying to trick you into giving up your personal information. The last thing you want is to find yourself the victim of tax identity theft. It's stressful and can take quite some time to clear up. Here are some of the scams out there now and how you can protect yourself.

Phone scams

Since 2013, phone scammers have defrauded at least 15,000 people in the U.S. of over \$300 million by calling taxpayers and pretending to be from the IRS or immigration authorities. They usually demand immediate payment by unorthodox methods such as a prepaid debit card, gift card (such as iTunes) or wire transfer. If you refuse to pay, they threaten you with arrest, deportation or suspension of your business or driver's license. They're unrelenting in their quest to dupe you and will often leave an urgent callback request if you don't answer. Scammers have the ability to make it look like their calls are coming from an actual IRS phone number and they may also use phony IRS badge numbers. Sometimes victims are also told they're getting a refund – this is another ploy to get your money and information.

Here's what you need to know – the IRS will never:

- Demand you pay your taxes with a gift card – this is a sure fire indication you are being scammed
- Threaten to immediately bring in police or other law enforcement agencies
- Say you have to pay without giving you the opportunity to question or appeal the amount they say you owe
- Ask for credit or debit card numbers over the phone
- Initiate contact with you by email or text message

If you receive a call like this, hang up immediately. Remember, scammers change their tactics, so even if the specifics of the call don't match these scenarios exactly, stay vigilant. One of the most recent iterations of this scam includes IRS impersonators demanding money from taxpayers for the nonexistent "Federal Student Tax." This scam surfaced after tax season, proving scammers go to great lengths year-round to try to deceive you. You can report scam phone calls to the IRS at www.tigta.gov and the FTC at www.ftc.gov.

Phishing

Phishing is an attempt to steal your identity via email. Scammers send out phony emails and create phony websites that look legitimate. They use names and logos to trick you into thinking you're receiving an official communication from the IRS or even tax software companies. These schemes can ask you about a wide range of topics to try to get your personal information such as refunds, filing status, ordering transcripts, etc. They may also include links to phony websites meant to install malware on your computer.

Another ploy to be on the lookout for – the Taxpayer Advocacy Panel (TAP) says some taxpayers have received emails

claiming to be from TAP about a tax refund. It's a scam. You can forward these emails to phishing@irs.gov. During the 2016 tax season, the IRS saw a 400% increase in phishing and malware scams. Here are some warning signs that the email you received is bogus:

- It's a reply to something you never sent or requested
- The sender is asking you to click on a link or open an attachment to avoid negative consequences or to receive something of value
- It was sent at an unusual time – like the middle of the night – instead of during regular business hours
- A hyperlink in the email – perhaps to a well-known website – is misspelled or missing characters. For example, irsgov instead of irs.gov.

Never open email attachments that end with .exe, .scr, .bat or .com; never click "unsubscribe" links and never reply to spam.

When in doubt about communications from the IRS, contact them directly or talk with your professional tax preparer.

Source: IRS

Phillip R. McCollum, Jr., CPA, JD, Partner, specializes in tax planning, consulting and compliance work for privately held businesses and their owners. You can reach him at (480) 839-4900 or PhilMc@hhcpa.com.