

# Robert W. Davis, C.P.A.

Certified Public Accountant

## IRS Tax Tip 2018-38

### Don't Fall for Scam Calls and Emails Posing as IRS

Scammers and cyberthieves continue to use the IRS as bait. The most common tax scams are phone calls and emails from thieves who pretend to be from the IRS. Scammers use the IRS name, logo, fake employee names and badge numbers to try to steal money and identities from taxpayers.

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 taxpayers owe money and demand payment right away. Other times, scammers will lie to taxpayers and say they're 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 an immediate payment. The IRS won't call taxpayers if they owe taxes without first sending a bill in the mail.
- Demand payment without allowing taxpayers to question or appeal the amount owed.
- Demand that taxpayers pay their taxes in a specific way, such as with a prepaid debit card.
- Ask for credit or debit card numbers over the phone.
- Threaten to contact local police or similar agencies to arrest taxpayers for non-payment of taxes.
- Threaten legal action, such as a lawsuit.

If taxpayers don't owe or don't think they owe any tax, and they receive an inquiry like this, 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. Add "IRS Telephone Scam" to the comments of your report.

In most cases, an IRS phishing scam is an unsolicited, fake email that claims to come from the IRS. 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 the thieves get what they're after, they use it to steal a victim's money and 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](mailto:phishing@irs.gov). Then delete it.
- Don't open any attachments or click on any links. They may have malicious code that will infect your computer.

#### More information:

[Report Phishing](#)

Share this tip on social media -- #IRSTaxTip: Don't Fall for Scam Calls and Emails Posing as IRS. <https://go.usa.gov/xnhdt>

804 Pier View Way, Suite 204, Oceanside, CA 92054 ▪ P.O. Box 820 Oceanside, CA 92049

PHONE (760) 434-7762 ▪ FAX (760) 966-7417

[bob.davis@cpabob.com](mailto:bob.davis@cpabob.com)

[www.cpabob.com](http://www.cpabob.com)