

Sample article for organizations to use to reach customers (524 word count)

Post the following article on your websites and/or use in other communication vehicles to help your customers know the signs of an email scheme.

Be on the lookout for email schemes

After seeing an approximate 400 percent surge in [phishing and malware](#) incidents so far this tax season, the Internal Revenue Service is reminding people to be on the lookout for [email schemes](#). Variations of these scams can be seen via text messages, and the communications are being reported in every section of the country.

Fraudsters are more frequently asking for personal tax information, which they can use to help file false tax returns.

The emails are designed to trick you into thinking these are official communications from the IRS or others in the tax industry, including tax software companies. The phishing schemes can ask you about a wide range of topics. Emails can seek information related to refunds, filing status, confirming personal information, ordering transcripts and verifying PIN information.

If you click on the links in these emails, you will be taken to sites designed to imitate an official-looking website, such as [IRS.gov](#). The sites ask for Social Security numbers and other personal information. The sites also may carry malware, which can infect your computer and allow criminals to access your files or track your keystrokes to gain information.

What should you look for?

You may receive an official-looking email from what appears to be an official source, such as the IRS or someone in the tax industry.

The underlying messages frequently ask you to update important information by clicking on a Web link. The links may be masked to appear to go to official pages, but they can go to a scam page designed to look like the official page. **You should not click on these links, but instead send the email to phishing@irs.gov.** Learn more by going to the [Report Phishing and Online Scams](#) page.

Recent email examples the IRS has seen include subject lines and underlying text referencing:

- Numerous variations about people's tax refund.
- Update your filing details, which can include references to Form W-2.
- Confirm your personal information.

- Get *my IP Pin*.
- Get *my E-file Pin*.
- Order a transcript.
- Complete your tax return information.

It's important to keep in mind the IRS generally does not initiate contact by email to request your personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.

Date: March 1, 2016

NOTE TO EDITOR: Below are links to help taxpayers learn more about tax scams and identity theft.

- [Taxes. Security. Together](#)
- [Publication 4524, Security Awareness for Taxpayers](#)
- [IRS Security Awareness Tax Tips](#)
- www.irs.gov/identitytheft
- [IRS and Partner Statements on the October 2015 Security Summit Meeting](#)
- [Fact Sheet 2016-1](#), IRS, States and Tax Industry Combat Identity Theft and Refund Fraud on Many Fronts
- [Fact Sheet 2016-2](#), IRS, States and Tax Industry Urge Taxpayers to Join the Effort to Combat Identity Theft
- [Fact Sheet 2016-3](#), IRS Identity Theft Victim Assistance: How It Works
- [Fact Sheet 2016-4](#), How New Identity Security Changes May Affect Taxpayers for 2016