COMPTROLLER of MARYLAND
Serving the People

**Peter Franchot**

---

# TAXPAYER *Tips*

## IRS Warns Taxpayers of Numerous Tax Scams Nationwide; Provides Summary of Most Recent Schemes

**ANNAPOLIS (December 8, 2016)** — As tax season approaches, the Internal Revenue Service, many states, including Maryland, and the tax industry remind taxpayers to be on the lookout for emerging tax scams related to identity theft and refund fraud.

Every tax season, there is an increase in schemes that target innocent taxpayers by email, by phone and online. The IRS and Security Summit partners remind taxpayers and tax professionals to be on the lookout for these deceptive schemes. This reminder is presented to taxpayers during the "National Tax Security Awareness Week." Some of the most prevalent IRS impersonation scams include:

- **Requesting fake tax payments:** The IRS has seen automated calls where scammers leave urgent callback requests telling taxpayers to call back to settle their "tax bill." These fake calls generally claim to be the last warning before legal action is taken. Taxpayers may also receive live calls from IRS impersonators. They may demand payments on prepaid debit cards, iTunes and other gift cards or wire transfer. The IRS reminds taxpayers that any request to settle a tax bill using any of these payment methods is a clear indication of a scam. (IR-2016-99)
- **Targeting students and parents and demanding payment for a fake "Federal Student Tax":** Telephone scammers target students and parents demanding payments for fictitious taxes, such as the "Federal Student Tax." If the person does not comply, the scammer becomes aggressive and threatens to report the student to the police to be arrested. (IR-2016-107)
- **Sending a fraudulent IRS bill for tax year 2015 related to the Affordable Care Act:** The IRS has received numerous reports of scammers sending a fraudulent version of CP2000 notices for tax year 2015. Generally, the scam involves an email or letter that includes the fake CP2000. The fraudulent notice includes a payment request that taxpayers mail a check made out to "I.R.S." to the "Austin Processing Center" at a Post Office Box address. (IR-2016-123)
- **Soliciting W-2 information from payroll and human resources professionals:** Payroll and human resources professionals should be aware of phishing

email schemes that pretend to be from company executives and request personal information on employees. The email contains the actual name of the company chief executive officer. In this scam, the "CEO" sends an email to a company payroll office employee and requests a list of employees and financial and personal information including Social Security numbers (SSN). (IR-2016-34)

- **Imitating software providers to trick tax professionals:** Tax professionals may receive emails pretending to be from tax software companies. The email scheme requests the recipient download and install an important software update via a link included in the e-mail. Upon completion, tax professionals believe they have downloaded a software update when in fact they have loaded a program designed to track the tax professional's key strokes, which is a common tactic used by cyber thieves to steal login information, passwords and other sensitive data. (IR-2016-103)
- **"Verifying" tax return information over the phone:** Scam artists call saying they have your tax return, and they just need to verify a few details to process your return. The scam tries to get you to give up personal information such as a SSN or personal financial information, including bank numbers or credit cards. (IR-2016-40)
- **Pretending to be from the tax preparation industry:** The emails are designed to trick taxpayers into thinking these are official communications from the IRS or others in the tax industry, including tax software companies. The phishing schemes can ask taxpayers about a wide range of topics. E-mails or text messages can seek information related to refunds, filing status, confirming personal information, ordering transcripts and verifying PIN information. (IR-2016-28)

If you receive an unexpected call, unsolicited email, letter or text message from someone claiming to be from the IRS, here are some of the telltale signs to help protect yourself.

If you get a suspicious phone call from someone claiming to be from the IRS and asking for money, here's what you should do:

- Do not give out any information. Hang up immediately.
- Search the web for telephone numbers scammers leave in your voicemail asking you to call back. Some of the phone numbers may be published online and linked to criminal activity.
- Contact TIGTA to report the call. Use their "IRS Impersonation Scam Reporting" web page or call 800-366-4484.
- Report it to the Federal Trade Commission. Use the "FTC Complaint Assistant" on FTC.gov. Please add "IRS Telephone Scam" in the notes.
- If you think you might owe taxes, call the IRS directly at 800-829-1040.

If you receive an unsolicited email that appears to be from either the IRS or an organization closely linked to the IRS, such as the Electronic Federal Tax Payment System (EFTPS), report it by sending it to phishing@irs.gov.

###