Rhode Island Department of Revenue
Division of Taxation

ADV 2016-26
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
DECEMBER 6, 2016

Avoiding phishing scams helps to prevent identity theft

Security awareness tip from Internal Revenue Service and Rhode Island Division of Taxation

Simply ask for it. That's the easiest way for an identity thief to steal your personal information.

Each day, people fall victim to phishing scams through emails, texts, or phone calls and mistakenly turn over important data. In turn, cybercriminals try to use that data to file fraudulent tax returns or commit other crimes.

The Internal Revenue Service, state tax agencies, and the tax industry – all partners in the fight against identity theft – urge you to learn to recognize and avoid phishing scams.

We need your help in the fight against identity theft. That's why, as part of the Security Summit effort, we launched a public awareness campaign that we call Taxes. Security. Together. We've launched a series of security awareness tips that can help protect you from cybercriminals.

It's called "phishing" because thieves attempt to lure you into the scam mainly through impersonations. The scam may claim to be from a friend, a company with whom you do business, a prize award – anything to get you to open the email or text.

A good general rule: Don't give out personal information based on an unsolicited email request.

Here are a few basic tips to recognize and avoid a phishing email:

- **It contains a link.** Scammers often pose as the IRS, financial institutions, credit card companies, or even tax companies or software providers. They may claim they need you to update your account or ask you to change a password. The email offers a link to a spoofing site that may look similar to the legitimate official website. Do not click on the link. If in doubt, go directly to the legitimate website and access your account.
- **It contains an attachment.** Another option for scammers is to include an attachment to the email. This attachment may be infected with malware that can download malicious software onto your computer without your knowledge. If it's spyware, it can track your keystrokes to obtain information about your passwords, Social Security number, credit cards, or other sensitive data. Do not open attachments from sources unknown to you.

- **It's from a government agency.** Scammers attempt to frighten people into opening email links by posing as government agencies. Thieves often try to imitate the IRS and other government agencies.
- **It's an "off" email from a friend.** Scammers also hack email accounts and try to leverage the stolen email addresses. You may receive an email from a "friend" that just doesn't seem right. It may be missing a subject for the subject line or contain odd requests or language. If it seems off, avoid it and do not click on any links.
- **It has a lookalike URL.** The questionable email may try to trick you with the URL. For example, instead of www.irs.gov, it may be a false lookalike such as www.irs.gov.maliciousname.com. You can place your cursor over the text in such an email to view a pop-up of the real URL.
- **Use security features.** Your browser and email provider generally will have anti-spam and phishing features. Make sure you use all of your security software features.

Opening a phishing email and clicking on the link or attachment is one of the most common ways thieves are able not just to steal your identity or personal information, but also to enter into computer networks and create other mischief.

Learning to recognize and avoid phishing emails – and sharing that knowledge with your family members – is critical to combating identity theft and data loss. Businesses should educate employees about the dangers.

The IRS, state tax agencies, and the tax industry have joined as the Security Summit to implement a series of initiatives to help protect you from tax-related identity theft in 2017. The Security Summit partners recently announced "National Tax Security Awareness Week." As part of the Security Summit effort, the IRS, the states, and the tax community will share a variety of information throughout this week to educate taxpayers on steps they should take to protect themselves from identity theft and tax scams as well as protect their valuable financial data in advance of the upcoming filing season.

To learn more about protecting your personal and financial data, see: https://www.irs.gov/individuals/taxes-security-together.

See also IRS Publication 4524, "Security Awareness for Taxpayers," using the following link: https://www.irs.gov/pub/irs-pdf/p4524.pdf.

FOR MORE INFORMATION

To reach the Rhode Island Division of Taxation, call the Division's main phone line at (401) 574-8829. The Division is normally open to the public from 8:30 a.m. to 3:30 p.m. business days, and is located at One Capitol Hill in Providence, in the Powers Building, which is diagonally across Smith Street from the State House. For forms, instructions, and other information, see the Division website: www.tax.ri.gov. To reach specific sections with the agency, by phone or email, use the following address: www.tax.ri.gov/contact/