Rhode Island Department of Revenue
Division of Taxation

ADV 2018-15
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
APRIL 9, 2018

Security Summit warns taxpayers, tax professionals, about scam

New email version of scam is used by cybercriminals to trick people into opening links

PROVIDENCE, R.I. – With the April 17 tax deadline approaching, the Rhode Island Division of Taxation, the Internal Revenue Service, and other partners in the Security Summit today urged taxpayers and tax professionals to be alert to identity theft scams, especially a new email version currently pretending to be from “IRS Refunds.”

The “IRS Refunds” scam is a common tactic used by cybercriminals to trick people into opening a link or attachment associated with the email. The link takes people to a fake page where thieves try to steal personally identifiable information, such as Social Security numbers.

Often these links or attachments also secretly download malware that can perform many functions, such as giving the thief control of the computer or tracking keystrokes to determine other sensitive passwords or critical data.

Neither the IRS nor the Rhode Island Division of Taxation randomly contacts taxpayers or tax professionals via email. Neither agency asks people to confirm their tax refund information. The Division of Taxation and the IRS initiate most contacts through regular mail delivered by the U.S. Postal Service.

(There are special circumstances in which the IRS or the Division of Taxation will call or come to a home or business, such as when a taxpayer has an overdue tax bill, to secure a delinquent tax return or a delinquent employment tax payment, or to tour a business as part of an audit or during criminal investigations. Even then, however, taxpayers will generally first receive several letters – called “notices” – from the Division of Taxation or the IRS in the mail.)

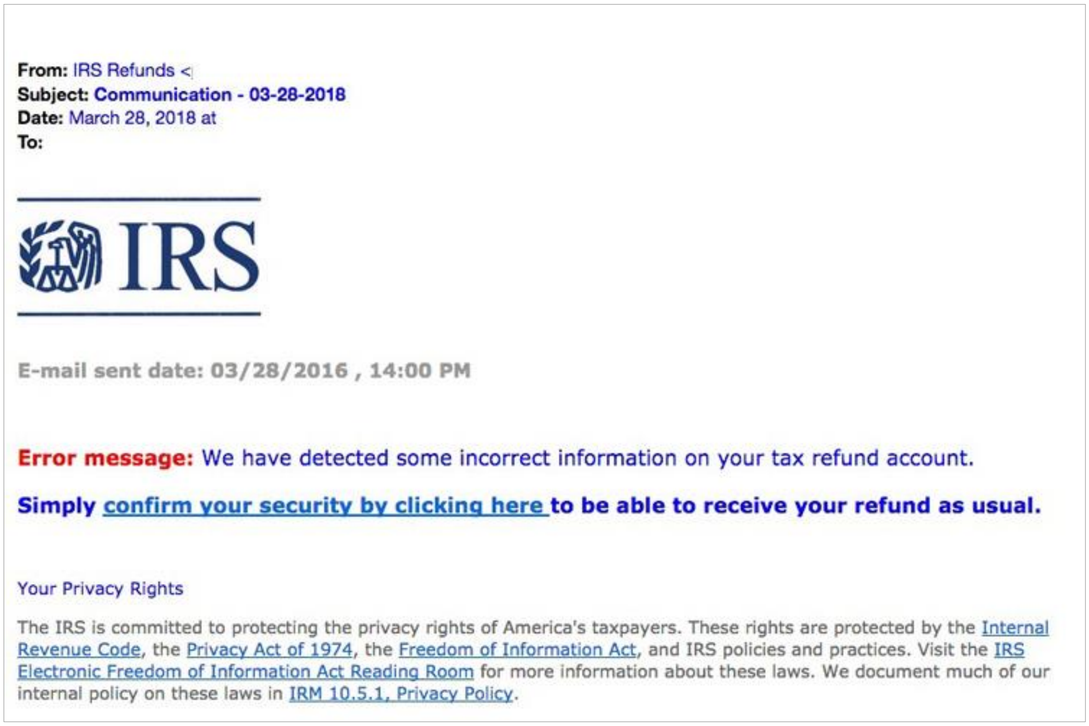
TAKE PRECAUTIONS

With scams like these circulating, taxpayers and tax professionals should take ongoing security precautions to protect their identities and their computer networks from identity thieves. Following are a few basic security steps for taxpayers:

- Always use security software with firewall and anti-virus protections.
- Make sure the security software is always turned on and can automatically update.
- Encrypt sensitive files such as tax records stored on computers.
- Use strong, unique passwords for each account.

- Learn to recognize and avoid phishing emails, threatening calls and texts from thieves posing as legitimate organizations such as banks, credit card companies, and even the IRS or the Division of Taxation.
- Do not click on links or download attachments from unknown or suspicious emails.
- Protect personal data. Don’t routinely carry Social Security cards, and make sure tax records are secure. Shop at reputable online retailers.
- Treat personal information like cash; don’t leave it lying around.

The latest email version of a scam may look like the image below:



From: IRS Refunds <

Subject: **Communication - 03-28-2018**

Date: March 28, 2018 at

To:

E-mail sent date: 03/28/2016 , 14:00 PM

Error message: We have detected some incorrect information on your tax refund account.

Simply confirm your security by clicking here to be able to receive your refund as usual.

Your Privacy Rights

The IRS is committed to protecting the privacy rights of America's taxpayers. These rights are protected by the Internal Revenue Code, the Privacy Act of 1974, the Freedom of Information Act, and IRS policies and practices. Visit the IRS Electronic Freedom of Information Act Reading Room for more information about these laws. We document much of our internal policy on these laws in IRM 10.5.1, Privacy Policy.

Following are a few basic security steps for tax professionals:

- Learn to recognize phishing emails, especially those pretending to be from the IRS, e-Services, a tax software provider, or cloud storage provider.
- Never open a link or any attachment from a suspicious email. Remember: Neither the IRS nor the Division of Taxation initiates initial contact with tax pros via email.
- Create a data security plan using IRS Publication 4557, “Safeguarding Taxpayer Data”, and Small Business Information Security – The Fundamentals, by the National Institute of Standards and Technology.
- Review internal controls:
    - Install anti-malware/anti-virus security software on all devices (laptops, desktops, routers, tablets, and phones) and keep software set to automatically update.
    - Use strong and unique passwords of 10 or more mixed characters; password-protect all wireless devices; and use a phrase or words that are easily remembered and change passwords periodically.
    - Encrypt all sensitive files/emails and use strong password protections.

- Back-up sensitive data to a safe and secure external source not connected fulltime to a network.
- Wipe clean or destroy old computer hard drives that contain sensitive data.
- Limit access to taxpayer data to individuals who need to know.
- Check IRS e-Services account weekly for number of returns filed with EFIN.

ABOUT THE SECURITY SUMMIT

The IRS, state tax agencies, and the tax industry, working together as the Security Summit, have made significant strides in fighting identity theft and data theft. But cybercriminals continue to evolve and Summit partners need the help of everyone, including tax professionals and taxpayers, to continue this progress. To learn more, click here.