Tax Filing Season, Important Points

Introduction

- We will soon be entering the tax filing season and need to be aware of tax scams **and** schemes.
- In recent years, thousands of people have lost millions of dollars and their personal information to tax scams and fake IRS communication.
- REMEMBER: The IRS doesn't initiate contact with taxpayers by email, text messages or social media channels to request personal or financial information.
- Additionally, IRS does not threaten taxpayers with lawsuits, imprisonment or other enforcement action**s.** Being able to recognize these tell-tale signs of a phishing or tax scam could save you from becoming a victim.
- If it sounds too good to be true, it probably is!

Identity Theft

- The IRS combats tax-related identity theft with an aggressive strategy of prevention, detection and victim assistance. We're making progress against this crime, and it remains one of our highest priorities. If you become a victim, we're committed to helping you resolve your case as quickly as possible.

- IRS Criminal Investigation (CI) detects and investigates tax fraud and other financial fraud, including fraud related to identity theft. Identity theft is often found through our Questionable Refund Program (QRP) area where we detect false returns which may have used stolen identities to claim fraudulent tax refunds. Additional areas involving identity theft include employment tax cases, abusive return preparer schemes, and narcotics and money laundering investigations.

- Learning you are a victim of identity theft can be a stressful event. Identity theft is also a challenge to businesses, organizations and government agencies, including the IRS.

- Many times, you may not be aware that someone has stolen your identity. The IRS may be the first to let you know you're a victim of ID theft after you try to file your taxes.

- Here are ten things to know about ID Theft:
    - **Protect your Records.** Do not carry your Social Security card or other documents with your SSN on them. Only provide your SSN if it's necessary and you know the person requesting it. Protect your personal information at home and protect your computers with anti-spam and anti-virus software. Routinely change passwords for Internet accounts.

    - **Don't Fall for Scams.** The IRS will not call you to demand immediate payment, nor will it call about taxes owed without first mailing you a bill. Beware of threatening phone calls from someone claiming to be from the IRS. If you have no reason to believe you owe taxes, report the incident to the Treasury Inspector General for Tax Administration (TIGTA) at 1-800-366-4484.

    - **Report ID Theft to Law Enforcement.** If your SSN was compromised and you think you may be the victim of tax-related ID theft, file a police report. You can also file a report with the Federal Trade Commission using the FTC Complaint Assistant. It's also important to contact one of the three credit bureaus so they can place a freeze on your account.

    - **Complete an IRS Form 14039 Identity Theft Affidavit.** Once you've filed a police report, file an IRS Form 14039 Identity Theft Affidavit. Print the form and mail or fax it

according to the instructions. Continue to pay your taxes and file your tax return, even if you must do so by paper.

- **Understand IRS Notices.** Once the IRS verifies a taxpayer's identity, the agency will mail a particular letter to the taxpayer. The notice says that the IRS is monitoring the taxpayer's account. Some notices may contain a unique Identity Protection Personal Identification Number (IP PIN) for tax filing purposes.

- **IP PINs.** If a taxpayer reports that they are a victim of ID theft or the IRS identifies a taxpayer as being a victim, they will be issued an IP PIN. The IP PIN is a unique six-digit number that a victim of ID theft uses to file a tax return.

- **Data Breaches.** If you learn about a data breach that may have compromised your personal information, keep in mind not every data breach results in identity theft. Further, not every identity theft case involves taxes. Make sure you know what kind of information has been stolen so you can take the appropriate steps before contacting the IRS.

- **Report Suspicious Activity.** If you suspect or know of an individual or business that is committing tax fraud, you can visit IRS.gov and follow the chart on How to Report Suspected Tax Fraud Activity.

- **Combating ID Theft.** Over the past few years, more than 2,100 people have been sentenced in connection with refund fraud related to identity theft. In FY 2016 the average prison sentence was 40 months.

- **Service Options.** Information about tax-related identity theft is available online. We have a special section on IRS.gov devoted to identity theft and a phone number available for victims to obtain assistance.

Return Preparer Fraud

- Preparing your tax return is often a task few embrace. For many, simple tax return preparation can be complex and requires time to understand. The help of a tax preparer is often the solution many choose to complete those forms. A tax preparer is a person you trust with your financial life to help you comply with the law.

- IRS Criminal Investigation (CI) reminds you;
  - Taxpayers are responsible for the accuracy of all entries made on their tax returns, whether the return is prepared by the taxpayer or by a return preparer.
  - Be careful in selecting the tax professional who will prepare your return. Some basic tips and guidelines to assist taxpayers in choosing a reputable tax professional are:
    - Avoid return preparers who claim they can obtain larger refunds than other preparers.
    - Avoid preparers who base their fee on a percentage of the amount of the refund.
    - Use a reputable tax professional that signs and enters a preparer tax identification number (PTIN) on your tax return and provides you with a copy for your records.
    - Consider whether the individual or firm will be around to answer questions about the preparation of your tax return, months, even years, after the return has been filed.
    - Never sign a blank tax form.
    - Ask questions. Do you know anyone who has used the tax professional? Were they satisfied with the service they received?

- **Tax Evasion is a crime**, a felony, punishable up to 5 years imprisonment and a $250,000 fine.

Scams and Schemes

The three most common types of scams that the IRS is seeing are:

- **IRS-Impersonation Telephone Scams**
  - An aggressive and sophisticated phone scam targeting taxpayers, including recent immigrants, has been making the rounds throughout the country. Callers claim to be employees of the IRS, but are not. These con artists can sound convincing when they call. They use fake names and bogus IRS identification badge numbers. They may know a lot about their targets, and they usually alter the caller ID to make it look like the IRS is calling.
  - Victims are told they owe money to the IRS and it must be paid promptly through a pre-loaded debit card or wire transfer. If the victim refuses to cooperate, they are then threatened with arrest, deportation or suspension of a business or driver's license. In many cases, the caller becomes hostile and insulting. Or, victims may be told they have a refund due to try to trick them into sharing private information. If the phone isn't answered, the scammers often leave an "urgent" callback request.
  - **Remember:** Scammers Change Tactics -- Aggressive and threatening phone calls by criminals impersonating IRS agents remain a major threat to taxpayers, but variations of the IRS impersonation scam continue year-round and they tend to peak when scammers find prime opportunities to strike.

- **Surge in Email, Phishing and Malware Schemes**
  - The IRS saw an approximate 400 percent surge in phishing and malware incidents in the 2016 tax season.
  - Scam 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. These phishing schemes can ask taxpayers about a wide range of topics. Emails can seek information related to refunds, filing status, confirming personal information, ordering transcripts and verifying PIN information.
  - Variations of these scams can be seen via text messages, and the communications are being reported in every section of the country.
  - When people click on these email links, they are 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, which could be used to help file false tax returns. The sites also may carry malware, which can infect people's computers and allow criminals to access your files or track your keystrokes to gain information.

- **Email Phishing Scam: "Update your IRS e-file"**
  - The IRS is aware of email phishing scams that appear to be from the IRS and include a link to a bogus web site intended to mirror the official IRS web site. These emails contain the direction "you are to update your IRS e-file immediately." The emails mention USA.gov and IRSgov (without a dot between "IRS" and "gov"), though notably, not IRS.gov (with a dot). Don't get scammed. These emails are not from the IRS.
  - Remember, the IRS does not initiate contact with taxpayers by email to request personal or financial information.

Other Recent Tax Scams

- Fake emails purporting to contain an IRS tax bill related to the Affordable Care Act. Generally, the scam involves an email that includes a fraudulent version of CP2000 notices for tax year 2015 as an attachment.
- Telephone scammers targeting students and parents during the back-to-school season and demanding payments for non-existent 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.
- The IRS has seen an increase in “robo-calls” where scammers leave urgent callback requests through the phone 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. In the latest trend, IRS impersonators are demanding payments on iTunes and other gift cards.
- This variation tries to play off the current tax season. Scammers 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 Social Security number or personal financial information, such as bank numbers or credit cards.

Don’t be a victim! Visit www.irs.gov for the latest information on new scams and schemes!