From the office of
Information Technology

Fraud Alert! Beware of Common Tax Scams

Tax season is upon us, a time of year when the scammers go into overdrive. Be extra careful while online, and avoid activities that could put your identity and finances at risk. It doesn't matter whether you owe money to the IRS or are expecting a refund, as the scammers will target you regardless of your situation.

Let's explore some common tax scams, warning signs that you may be victim, and steps you can take to protect yourself, your identity, and your finances.

Common Tax Scams

Cyber criminals use the same tried-and-true methods for tax scams as they do with other targeted attacks.

- **Phishing:** This tactic involves using email or malicious websites to infect your device or trick you into disclosing your information. Phishing emails may appear to come from real financial institutions, e-commerce sites, charitable organizations, or even government agencies such as the IRS.
- **Phone Calls:** This tactic involves making phone calls or leaving voicemails of an urgent or threatening nature. In the case of tax scams, the calls may advise you of a refund you are owed or demand that you settle an outstanding payment for back taxes. Caller ID spoofing may be used, making it appear like the person calling is from the IRS.

Scammers using these tactics generally attempt to create a sense of urgency, or have a good story that would tend to compel you to disclose personal information such as such as your date of birth, social security number, driver's license number, or even usernames and passwords to your accounts. Watch out for these common scams:

- **Refund Calculation Scam:** "The IRS recalculated your refund. Congratulations, we found an error in the original calculation of your tax return and owe you additional money. Please verify your account information so we can make a deposit."
- **Stimulus Payment Scam:** "Our records show that you have not claimed your COVID-19 stimulus payment. Please provide us with your information so we can send it to you."
- **Verification Scam:** "We need to verify your W-2 and other personal information. Please take pictures of your driver's license, documents, and forms and send them to us."
- **Gift Card Scam:** "You owe us back taxes and may be charged with a federal crime. You must pay a penalty to avoid being prosecuted. Purchase these gift cards and send them to us and we will wipe your

record clean."

- **Fake Charity Scam:** Scammers pose as a legitimate charity, often with a similar name as a real charity, to trick you into donating money to their own cause–filling their pockets.
- **Fake Tax Preparers:** Watch out for tax preparers that refuse to sign the returns they prepare. If they gain access to your information, they may file fraudulent tax returns redirecting your refund or attempt to access your bank accounts.

Warning Signs

Hopefully you have avoided the common tax scams, but the cyber criminals may have other methods of obtaining your information, such as data breaches of companies you do business with. Watch out for these warning signs that you may already be a victim.

- You attempt to file a tax return, either online or by mail, but are informed by the IRS or your state that they have already received one.
- You are informed by the IRS that an account has been registered in your name at IRS.gov even though you have never created one.
- You receive a transcript from the IRS that you did not request.

How to Protect Yourself

- **Identity Theft Resources**
  - If you believe you have become a victim of Identity Theft, visit IdentityTheft.gov to report it and create a recovery plan.
  - For specific information and resources for tax-related identity theft, visit the Identity Theft Central web page on the IRS web site.
- **E-mail and Internet Security Best Practices**
  - Never use public Wi-Fi to file your taxes or conduct other business such as online banking. Only connect to networks that you trust.
  - Remember that IRS.gov is the only genuine website for the Internal Revenue Service. All Internet and email communications between you and the IRS would be through this site.
  - Never send sensitive information via email. If you receive an email from an unknown source or one that seems suspicious, do not reply.
  - Report tax-related phishing emails to Phishing@IRS.gov. Visit Tax Scams - How to Report Them on the IRS web site for additional information.
- **IRS Representatives – Know How They Operate**
  - The first point of contact by the IRS is typically via postal mail. The IRS will not contact you via email, text messaging, or your social network, nor does it advertise on websites.
  - IRS representatives always carry two forms of official credentials, and you can confirm their identity by calling a dedicated IRS telephone number for verification.
  - The IRS does not accept payments by gift cards.
  - Review How to know it's really the IRS calling or knocking on your door on the IRS web site for additional information.
- **Donating to Charities**
  - Only donate to charitable organizations that you trust. Beware of charities that require you to give or send cash.
  - Verify charitable organizations using the Tax-Exempt Organization

Search web page on the IRS web site.

- **Using Tax Preparers**
  - Beware of tax preparers that only accept cash payments or offer to claim fake deductions to inflate your tax refund.
  - Only use a preparer that can provide you with their Tax Preparer Identification. You can verify your tax preparer through the Directory of Federal Tax Return Preparers with Credentials and Select Qualifications on the IRS web site.
  - Visit Topic No. 254 How to Choose a Tax Return Preparer for best practices on selecting your tax preparer.
- **Secure Your Identity**
  - Get An Identity Protection PIN (IP PIN) from the IRS to prevent someone else from filing a tax return in your name.
  - Check with your state to see if they offer a similar program to file your state taxes.