TAX YEAR
2022

Tax Scams—Protect Yourself

www.phbcpa.com

PHB Certified Public Accountants
Piehl Hanson Beckman

Tax Scams – Protect Yourself

There are many tax scams out there with the purpose of stealing your identity, stealing your money, or filing fraudulent tax returns using your private information. Tax scammers work year-round, not just during tax season and target virtually everyone. Stay alert to the ways criminals pose as the IRS to trick you out of your money or personal information.

The best thing to remember to protect yourself is that the IRS will never initiate contact with you via telephone, text message, email, or social media to request personal or financial information. The IRS will always first send a letter requesting information.

IRS-Impersonation Telephone Scam

An aggressive and sophisticated telephone 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 from information gathered from online resources, and they usually alter the caller ID (caller ID spoofing) to make it look like the IRS is calling. Also, if the phone is not answered, the scammers often leave an urgent callback request.

Victims are often told they owe money to the IRS and it must be paid promptly through a pre-loaded debit card, gift 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.

Alternatively, victims may be told they have a refund due to try to trick them into sharing private financial information.

You should note that the IRS will never:

- Call to demand immediate payment, nor will the agency call about taxes owed without first having mailed you a bill.
- Demand that you pay taxes without giving you the opportunity to question or appeal the amount they say you owe.
- Require you to use a specific payment method for your taxes, such as a prepaid debit card.
- Ask for credit card, debit card, or PIN numbers over the phone.
- Threaten to bring in local police or other law-enforcement groups to have you arrested for not paying.

What to do. If you receive a phone call from someone claiming to be from the IRS and asking for money, take the following steps.

- Do not provide any information to the caller. Hang up immediately.
- If you know you owe tax, or think you might owe, you should call the IRS at 1-800-829-1040 where you can get help with a payment issue.
- If you know you do not owe any tax, or have no reason to believe that you do, report the incident to TIGTA (Treasury Inspector General for Tax Administration) at 1-800-366-4484 or at www.tigta.gov.
- You should also contact the Federal Trade Commission and use the "FTC Complaint Assistant" at www.ftc.gov. When filing the complaint, add "IRS Telephone Scam" to the comments.

Tax Scams—Protect Yourself

Phony IRS Emails—"Phishing"

Scammers copy official IRS letterhead to use in emails they send to victims. Emails direct the consumer to a web link that requests personal and financial information, such as a Social Security Number, bank account, or credit card numbers. The practice of tricking victims into revealing private personal and financial information over the internet is known as "phishing."

The IRS does not notify taxpayers of refunds or payments due via email. Additionally, taxpayers do not have to complete a special form or provide detailed financial information to obtain a refund. Refunds are based on information contained on the federal income tax return filed by the taxpayer. The IRS never asks people for the PIN numbers, passwords, or similar secret access information for their credit card, bank, or other financial accounts.

What to do. If you receive an email from someone claiming to be from the IRS and asking for money, take the following steps:

- Do not reply to the email message.
- Do not give out your personal or financial information over email.
- Do not open any attachments or click on any of the links. They may have a malicious code that will infect your computer.
- Forward the email to the IRS at phishing@irs.gov.
- Delete the email.

Other Scams

Fake charities. Be on guard against groups masquerading as charitable organizations to attract donations from unsuspecting contributors. You should always check out a charity before you donate and should not feel pressured to give immediately. IRS.gov has the tools you need to check out the status of charitable organizations.

Offer in Compromise (OIC) mills. The IRS has the authority to settle federal tax liabilities by accepting less than full payment under certain circumstances. OIC mills contort the IRS program into something it is not. They mislead people who have no chance of meeting the requirements while charging excessive fees. Companies advertising on TV or radio frequently cannot do anything for you that you cannot do for yourself by contacting the IRS directly. Beware of promoters claiming their services are needed to settle with the IRS, that tax debt can be settled for "pennies on the dollar," or that there is a limited window of time to resolve tax debts with an OIC.

Social media scams. Beware of social media scams which frequently use events like COVID-19 to try to trick people. Any information that is publicly shared on social media platforms can be collected and used against you. Cons may also send emails impersonating your family, friends, or co-workers.

Ways to Protect Yourself From Scams

There are many precautions you can take to protect yourself from becoming a victim. These include:

- Personal information should not be provided over the phone, through the mail, or on the internet unless the taxpayer initiated the contact or is sure he or she knows with whom he or she is dealing.
- Social Security cards or any documents that include your Social Security Number (SSN) or individual taxpayer identification number (ITIN) should not be carried around.
- Do not give a business your SSN or ITIN just because they ask—provide it only if required.
- Financial information should be protected. Do not give out any financial information over the phone or via email.
- Credit reports should be checked yearly.
- You should review your Social Security Administration earnings statements annually.
- Protect personal computers by using firewalls and anti-spam/virus software, updating security patches and changing passwords for internet accounts.
- Review privacy settings on social media and limit data that is publicly shared.
- Report any instances of tax scams to the IRS.

Contact Us

There are many events that occur during the year that can affect your tax situation. Preparation of your tax return involves summarizing transactions and events that occurred during the prior year. In most situations, treatment is firmly established at the time the transaction occurs. However, negative tax effects can be avoided by proper planning. Please contact us in advance if you have questions about the tax effects of a transaction or event, including the following:

- Pension or IRA distributions.
- Significant change in income or deductions.
- Job change.
- Marriage.
- Attainment of age 59½ or 72.
- Sale or purchase of a business.
- Sale or purchase of a residence or other real estate.
- Retirement.
- Notice from IRS or other revenue department.
- Divorce or separation.
- Self-employment.
- Charitable contributions of property in excess of $5,000.