Protect yourself from fraudsters impersonating the IRS and other tax scams

Tax scammers continue to target taxpayers through email, text messages, phone calls and regular mail. They often try to create urgency or fear to trick victims into sharing sensitive information or sending money. The IRS warns taxpayers to remain cautious because scammers continually change tactics to steal personal and financial information.

IRS impersonation scams

First and foremost, know that the IRS will never contact you by email, text or social media channels about a tax bill or refund. Most IRS initial communications are sent through regular mail. So if you get a call or message saying it's the IRS and asking for your Social Security number, it's someone trying to steal your identity and defraud you. Remember that the IRS already has your Social Security number.

Here are some common impersonation-related schemes to be aware of:

Phone calls. AI-generated voices and spoofed caller IDs to impersonate IRS agents are becoming more common. Scammers may leave urgent messages threatening arrest, penalties or legal action unless immediate payment is made. The IRS stresses that it won't demand immediate payment over the phone.

Text messages and emails. Scammers use text messages and emails containing fake IRS links or QR codes to direct taxpayers to fraudulent websites designed to steal

personal or financial information. These messages often claim there's a problem with a refund, tax return or IRS account to try to create panic and pressure taxpayers into responding quickly.

Fake IRS notices. One current scheme takes advantage of growing confusion about the IRS CP53E notice. This is a notice related to tax refunds and bank account information. As the IRS shifts from paper checks to direct deposit, it's mailing these notices to taxpayers who may need to add or update their banking details. Unfortunately, the IRS is sometimes mistakenly sending the notices when a taxpayer has already provided this information, creating confusion. Now fraudsters are sending fake versions of the notice in an attempt to steal taxpayers' sensitive information. If you receive an IRS CP53E notice, verify its authenticity before acting. Don't click links or scan QR codes.

Malware. In scams to infect computers and phones with malicious software, a phony email claims to come from the IRS. The subject line often states that the message is a notice of underreported income or a refund. There may be an attachment or a link to a bogus web page with your "tax statement." When you open the attachment or click on the link, malware is downloaded to your device. This malware can give criminals remote access to your device and allow them to search for passwords, banking information and other sensitive data to help them steal your assets or your identity.

Other tax scams

The IRS recommends that taxpayers create an account to securely access their tax information. The account lets you view your refund status, make payments, check your balance and more. But be cautious. Scammers may offer account setup "help" so they can collect your sensitive data. Or they may use stolen personal information to access your account without authorization. Once inside an account, they may attempt to redirect refunds, obtain tax records or use the information to commit additional identity theft. Create and always access your account directly through IRS.gov, don't share your information with unsolicited third parties, and check your account regularly.

Also watch out for fake online tax deduction calculators. These digital tools are intended to steal personal information and money from unsuspecting users. They're often accompanied by false promises about new or expanded tax credits and deductions. The IRS says you should use calculators only on sites that end in .gov (such as irs.gov) or of well-known tax software companies. Also, be wary of any calculator that guarantees its result. Legitimate calculators can only produce estimates. And, as always, be suspicious of claims that seem "too good to be true," such as unusually large tax savings.

The IRS also warns taxpayers to avoid other schemes involving questionable refund claims or credits promoted online or through social media. Promoters may encourage taxpayers to file inaccurate forms or claim credits they don't qualify for. Improper claims can lead to refund delays, audits, penalties and other enforcement actions.

Reporting fraud

The IRS has launched a "Report fraud" webpage to simplify confidential reporting of suspected tax fraud or scams. It consolidates multiple IRS fraud-reporting options into a single location, allowing taxpayers to report suspected scams, tax evasion or other tax-related misconduct in one place: irs.gov/help/report-fraud.

If you've been a victim of identity theft, consider obtaining an Identity Protection Personal Identification Number (IP PIN). Issued by the IRS, this unique six-digit number helps prevent criminals from filing a fraudulent tax return using your Social Security number. It's valid for one year and is automatically replaced after expiration. You can expect to receive a new one each year in mid-December to early January. You can apply online or get one at a Taxpayer Assistance Center. Once you receive your IP PIN, be sure to safeguard it. Use it only on Forms 1040.

Stay alert

Tax-related scams continue to evolve, so it's important to be cautious when receiving unexpected phone calls, messages or even letters involving taxes, refunds or financial information. If you receive a questionable communication related to a tax return we prepared, contact us before responding. We can also answer other questions you have about protecting yourself from tax-related fraud.