IRS

IRS warning: Scammers work year-round; stay vigilant

IR-2022-25, February 3, 2022

WASHINGTON — As the new year begins, the Internal Revenue Service reminds taxpayers to protect their personal and financial information throughout the year and watch out for IRS impersonation scams, along with other schemes, that try to trick people out of their hard-earned money.

These schemes can involve text message scams, e-mail schemes and phone scams. This tax season, the IRS also warns people to watch out for signs of potential unemployment fraud.

"With filing season underway, this is a prime period for identity thieves to hit people with realistic-looking emails and texts about their tax returns and refunds," said IRS Commissioner Chuck Rettig. "Watching out for these common scams can keep people from becoming victims of identity theft and protect their sensitive personal information that can be used to file tax returns and steal refunds."

The IRS, state tax agencies and the nation's tax industry – working together in the Security Summit initiative – have taken numerous steps since 2015 to protect taxpayers, businesses and the tax system from identity thieves. Summit partners continue to warn people to watch out for common scams and schemes this tax season.

Text message scams

Last year, there was an uptick in text messages that impersonated the IRS. These scams are sent to taxpayers' smartphones and have referenced COVID-19 and/or "stimulus payments." These messages often contain bogus links claiming to be IRS websites or other online tools. Other than IRS Secure Access, the IRS does not use text messages to discuss personal tax issues, such as those involving bills or refunds. The IRS also will not send taxpayers messages via social media platforms.

If a taxpayer receives an unsolicited SMS/text that appears to be from either the IRS or a program closely linked to the IRS, the taxpayer should take a screenshot of the text message and include the screenshot in an email to phishing@irs.gov with the following information:

- Date/time/time zone they received the text message
- Phone number that received the text message

The IRS reminds everyone NOT to click links or open attachments in unsolicited, suspicious or unexpected text messages – whether from the IRS, state tax agencies or others in the tax community.

Unemployment fraud

As a new tax season begins, the IRS reminds workers to watch out for claims of unemployment or other benefit payments for which they never applied. States have experienced a surge in fraudulent unemployment claims filed by organized crime rings using stolen identities. Criminals are using these stolen identities to fraudulently collect benefits.

Because unemployment benefits are taxable income, states issue Form 1099-G, Certain Government Payments, to recipients and to the IRS to report the amount of taxable compensation received and any withholding. Any worker receiving a fraudulent or inaccurate 1099-G should report it to the issuing state agency and request a corrected Form 1099-G.

For details on how to report fraud to state workforce agencies, how to obtain a corrected Form 1099-G, how to find a list of state contacts and other steps to take related to unemployment fraud, taxpayers can visit the U.S. Department of Labor's DOL.gov/fraud page.

Individuals may be victims of unemployment identity theft if they received:

- Mail from a government agency about an unemployment claim or payment for which they did not file. This includes unexpected payments or debit cards and could be from any state.
- An IRS Form 1099-G reflecting unemployment benefits they weren't expecting or didn't receive. Box 1 on this form may show unemployment benefits they did not receive or an amount that exceeds their records for benefits they did receive. The form itself may be from a state in which they did not file for benefits.

A notice from their employer indicating the employer received a request for information about an unemployment claim.

Email phishing scams

The IRS does not initiate contact with taxpayers by email to request personal or financial information. The IRS initiates most contacts through regular mail delivered by the United States Postal Service.

If a taxpayer receives an unsolicited email that appears to be from either the IRS or a program closely linked to the IRS that is fraudulent, report it by sending it as an attachment to phishing@irs.gov. The Report Phishing and Online Scams page at IRS.gov provides complete details.

There are special circumstances when the IRS will call or come to a home or business. These visits include times when a taxpayer has an overdue tax bill, a delinquent tax return or a delinquent employment tax payment. The IRS may also visit if it needs to tour a business as part of a civil investigation (such as an audit or collection case) or during a criminal investigation. The IRS provides specific guidance on how to know it's really the IRS knocking on your door.

Phone scams

The IRS does not leave pre-recorded, urgent or threatening messages. In many variations of the phone scam, victims are told if they do not call back, a warrant will be issued for their arrest. Other verbal threats include law-enforcement agency intervention, deportation or revocation of licenses.

Criminals can fake or "spoof" caller ID numbers to appear to be anywhere in the country, including from an IRS office. This prevents taxpayers from being able to verify the true call number. Fraudsters also have spoofed local sheriff's offices, state departments of motor vehicles, federal agencies and others to convince taxpayers the call

is legitimate.

The IRS (and its authorized private collection agencies) will never:

- Call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card or wire transfer. The IRS does not use these methods for tax payments.
- Threaten to immediately bring in local police or other law-enforcement groups to have the taxpayer arrested for not paying.
- Demand that taxes be paid without giving the taxpayer the opportunity to question or appeal the amount owed.
- Ask for credit or debit card numbers over the phone.

Generally, the IRS will first mail a bill to any taxpayer who owes taxes. All tax payments should only be made payable to the U.S. Treasury and checks **should never be made payable to third parties**.

For anyone who doesn't owe taxes and has no reason to think they do:

- Do not give out any information. Hang up immediately.
- Contact the Treasury Inspector General for Tax Administration to report the call at IRS Impersonation Scam Reporting.
- Report the caller ID and/or callback number to the IRS by sending it to phishing@irs.gov (Subject: IRS Phone Scam).
- Report it to the Federal Trade Commission on FTC.gov. Add "IRS Telephone Scam" in the notes.

For anyone who owes tax or thinks they do:

- View tax account information online at IRS.gov to see the actual amount owed. Taxpayers can also review their payment options.
- Call the number on the billing notice or
- Call the IRS at 800-829-1040. IRS employees can help.

Help for victims of ID theft

Unfortunately, scams and schemes can often lead to identity theft. While identity theft can have many consequences, the IRS focuses on tax-related identity theft.

Tax-related identity theft occurs when someone uses an individual's stolen Social Security number (SSN) to file a tax return claiming a fraudulent refund. Taxpayers may be unaware of this activity until they e-file a tax return and discover that a return has already been filed using their SSN. Or, the IRS may send them a letter saying it has identified a suspicious return using their SSN.

If a taxpayer learns their SSN has been compromised, or they know or suspect they are a victim of tax-related identity theft, the IRS recommends these additional steps:

- Individuals should respond immediately to any IRS notice; call the number provided.
- Taxpayers should complete IRS Form 14039, Identity Theft Affidavit PDF, if an e-file tax return rejects because of a duplicate filing under their SSN or they are instructed to do so by the IRS. Individuals can use a fillable form at IRS.gov, then print and attach the form to their paper return and mail according to instructions.

- Victims of tax-related identity theft should continue to pay their taxes and file their tax return, even if they must do so by paper.
- Taxpayers who previously contacted the IRS about tax-related identity theft and did not have a resolution should call for specialized assistance at 800-908-4490.

More information is available at: IRS.gov/identitytheft or the Federal Trade Commission's IdentityTheft.gov.

The official IRS website is IRS.gov. People should be aware of imitation websites ending in .com. This applies to other IRS tools, too, like Free File – they all end in .gov.

For more information, visit Tax Scams and Consumer Alerts on IRS.gov. Additional information about tax scams is available on IRS social media sites, including YouTube videos.

More information:

- Taxpayer Bill of Rights

Page Last Reviewed or Updated: 01-Mar-2022