IRS

Dirty Dozen: Scammers use every trick in their communication arsenal to steal your identity, personal financial information, money and more

IR-2022-121, June 8, 2022

WASHINGTON — Suspicious communications in all its forms designed to either trick, surprise or scare someone into responding before thinking is No. 7 on the 2022 "Dirty Dozen" scams warning list, the Internal Revenue Service announced today, warning everyone to be on the lookout for bogus calls, texts, emails and posts online to gain trust or steal.

Criminals have used these methods for years and they persist because these tricks work enough times to keep the scammers at it. Victims are tricked into providing sensitive personal financial information, money or other information. This can be used to file false tax returns and tap into financial accounts, among other schemes.

"If you are surprised or scared by a call or text, it's likely a scam so proceed with extreme caution," said IRS Commissioner Chuck Rettig. "I urge everyone to verify a suspicious email or other communication independently of the message in question."

The IRS has compiled the annual Dirty Dozen list for more than 20 years as a way of alerting taxpayers and the tax professional community about scams and schemes. The list is not a legal document or a literal listing of agency enforcement priorities. It is designed to raise awareness among a variety of audiences that may not always be aware of developments involving tax administration.

As part of the Security Summit effort with the states and the nation's tax industry, the IRS has made great strides in preventing and reducing tax-related identity theft. But it remains a serious threat to taxpayers and tax professionals who don't adequately protect Social Security numbers (SSN) and other personal information.

For example, criminals can quickly file a fake tax return using a stolen SSN in the hope that it has not already appeared on another filed return. People frequently don't know they are a victim of identity theft until they are notified by the IRS of a possible issue with their tax return or their return is rejected because the SSN appears on a return already filed.

Here are some common scams the IRS continues to see. Taxpayers should take extra caution with these schemes, which continue to evolve and change:

Text message scams: These scams are sent to taxpayers' smartphones and can reference things like 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 and 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.

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

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 caller's true 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. For more information, see IRS warning: Scammers work year-round; stay vigilant.

Page Last Reviewed or Updated: 09-Jun-2022