Cyndi Wilkinson, CPA - Tax Tips

July 2024

Beware of scammers posing as the IRS.

Email, Text and Social Media

The IRS will mail a letter or notice before calling or emailing.

The IRS **does not**:

- Send unexpected or unsolicited text messages to taxpayers.
- Initiate contact with taxpayers by email, text message or through social media.
- Send messages that ask for personal or financial information, especially when it comes to a tax refund.

Common IRS-related online scams include:

- Phishing email sent to you.
- Fake IRS social media accounts that contact you about a fake bill, grant or refund.
- Text messages sent to you for fake "tax credits" or "stimulus payments."

Scammers' messages often direct you to click fraudulent links they claim are IRS websites or other online tools.

Phone calls

After mailing a notice or letter to you, IRS agents may call to confirm an appointment or discuss items for a scheduled audit. You should know that:

- The IRS doesn't leave pre-recorded, urgent or threatening messages. Scammers will tell victims that if they do not call back, a warrant will be issued for their arrest. **These calls are scams**.
- Private collection agencies that the IRS works with may call you to collect certain outstanding inactive tax liabilities, but only after sending written notice to you and your representative.
- The IRS and its authorized private collection agencies will never ask you to pay using any form of pre-paid card, store or online gift card. You can review the IRS payments page at IRS.gov/payments for all legitimate ways to make a payment.

Letters and notices

A letter or notice is usually the first contact a taxpayer gets from the IRS contacts. If you get a suspicious letter or notice, you can check to see if it's really the IRS:

- Log in to your secure IRS Online Account (if you have one) to find a copy of the notice or letter.
- Contact IRS customer service to verify it, if aren't able to do so in your Online Account.
- Review IRS letters and notices at Understanding Your IRS Notice or Letter.
- Confirm that collection notices from a private collection agency have the same Taxpayer Authentication Number as the Notice CP40 you already received from the IRS.
- Visit Private Debt Collection Frequently Asked Questions to learn more about verifying a private collection agency.

Warning signs of a scam

If you get an unexpected letter, email or text that claims to be from the IRS or another trusted source – like a bank, a credit company or a tax software provider – here are some tell-tale signs that it's a scam:

- Spelling errors or incorrect grammar.
- A link or attachment that with a slightly misspelled URL or an unusual one such as irs.**com**. All IRS links go to irs.gov.
- A threatening or urgent request to pay now, to follow a link or to open an attachment.

Taxpayers who receive a request from IRS in the mail or by phone can always contact IRS customer service to authenticate