THE NORTHERN TRUST INSTITUTE

TAX NEWS YOU CAN USE

AVOIDING SCAMMERS POSING AS THE IRS

Jane G. Ditelberg
Director of Tax Planning, The Northern Trust Institute

Cybercrime of all kinds is on the rise, and with the 2024 tax return filing season in full swing, scams from bad actors posing as the Internal Revenue Service have also surged. According to cybersecurity company Guardio, in January there was a 77% increase in IRS scam messages.[1]

In many cases, criminals posing as IRS agents demand payments or personal information from taxpayers through emails, texts and phone calls. Some promise unclaimed refunds or resolution of past tax debt, or threaten large financial penalties, incarceration or other punitive measures. In other cases, identity thieves file false returns claiming refunds that belong to their victims.

The rise of generative AI has aided scammers in becoming even more sophisticated in their methods. In some cases, they may use the technology to impersonate your tax preparer or IRS agents, and their communications may contain other stolen personal information — such as your address or social security number — to make an email or letter appear to be official. There may be a sense of urgency to act immediately to avoid a penalty or to obtain a promised benefit.

Tips for distinguishing between legitimate and fraudulent communications from the

IRS

Understanding how the IRS legitimately contacts taxpayers can weed out many of the scams immediately. Knowing your rights and where to turn for assistance if a scam is suspected can help you avoid these traps and protect your identity and assets.

- The IRS never initiates contact with taxpayers by email, text message, messaging apps like WhatsApp or via social media. Virtually all initial contact from the IRS will be by U.S. mail or by a phone call requesting an appointment with an IRS agent.
- IRS agents do not request confidential information over the phone.
- IRS agents do not demand payment over the phone in any form. The IRS will send a taxpayer a written notice of deficiency, which is like a bill for taxes they have concluded the taxpayer owes. The taxpayer has the right to review and dispute the bill before paying it.
- IRS agents do not demand payment by credit or debit card, wire transfer, cash, gift cards, cryptocurrency or payment apps such as Venmo or CashApp. While a taxpayer may elect to pay via wire transfer or credit card, taxes can always be paid by check or money order payable to "United States Treasury."
- A request to deposit cash into a cryptocurrency ATM to pay taxes, fines or penalties is always fraudulent.
- If a return is selected for audit, the taxpayer may get a letter (or on occasion a phone call) to set up an appointment or a request for documents. An IRS agent will not ask a taxpayer for payment to "stop" the audit.
- Most taxpayers can now apply for an "IP PIN" from the IRS. IP stands for identity protector, and it is designed to prevent identity theft or the filing of fraudulent returns using a taxpayer's data. If a taxpayer has an IP PIN, they must use it on all returns filed that year, and any returns filed without the IP PIN (whether electronically or on paper) will automatically be rejected by the IRS.
- For more information regarding how and when the IRS contacts you, visit https://www.irs.gov/newsroom/how-to-know-if-its-really-the-irs

What about in-person visits from agents?

In certain cases, an IRS agent may make an in person visit. You should be aware of the tax issue prior to the visit because the IRS will first try to resolve the matter by mail. However, while on occasion the agent may make an appointment, other times the visit will be unannounced. A legitimate IRS agent will have two official forms of identification — an HSPD-12 card, which is the standard federal government credential, and a pocket commission. You have the right to see these and to verify the agent's identity by calling a dedicated IRS telephone number for verifying the agent. You may also request the name and telephone number of the agent's manager to verify the validity of the inquiry. Visit www.irs.gov for additional resources regarding verification of the identity of an agent or officer. If taxes are due, the agent will ask for payment. Taxes can always be paid by check or money order payable to the "United States Treasury."

Turn to experts you trust

If you receive a notice from the IRS that you have questions about, the best precaution is to contact your return preparer, advisor, attorney or accountant to review it before responding. These professionals have training and experience to review and understand any legitimate notice and help respond — as well as to help identify spoofs from scammers.

You can also consult www.irs.gov for consumer alerts. If you are concerned about an inquiry into a return you filed or a payment you made, you can create an account at https://www.irs.gov/individuals/get-transcript to review your tax transcript and confirm activity in your account. This can also be helpful if it appears an identity thief has filed tax documents using your personal information.

Simple guidelines to remember

Some commonsense rules can help identify scams in the tax arena and elsewhere.

- **Identify who the communication is actually from.** Addresses can be spoofed, and slight differences can trick the eye. For example, should you open an email from IRS.net? What about one from lRS.gov? Neither of those senders is legitimate — the first uses the incorrect domain (.net instead of .gov), and the second misspells IRS, using a lowercase L instead of an uppercase I.
- **Consider whether the request is reasonable.** Are you being asked to respond urgently with an irrevocable release of funds or information? Are you being asked to click on a link in an email or open an attachment? None of these actions are consistent with IRS communication protocols.
- **Does the communication contain an express or implied threat?** While you may feel apprehensive about any communication from the tax authorities, an IRS agent is not going to threaten bodily harm. You can report threats by requesting the agent's identification number or the name and telephone number of the agent's manager. Other options are available on the www.irs.gov website.
- **Things that sound too good to be true usually are.** If someone is promising to erase your back taxes, or offers a chance to avoid paying any income tax at all, be skeptical. When in doubt, contact your tax preparer or other legal or tax advisors to ensure that the inquiry is legitimate.

Additional resources

The IRS has issued numerous consumer alerts regarding scams, and their website has information about avoiding, identifying, and reporting scams.

- To view recent consumer alerts, visit https://www.irs.gov/newsroom/tax-scamsconsumer-alerts.
- To report a phishing or vishing scam, email phishing@irs.gov.
- To verify the identity of someone who contacts you purporting to be from the IRS, contact IRS customer service. For more information, visit https://www.irs.gov/help/let-us-help-you.

1. https://www.newsweek.com/irs-scam-messages-surge-what-do-if-you-get-one-2033912

Disclosures

This information is not intended to be and should not be treated as legal, investment, accounting or tax advice and is for informational purposes only. Readers, including professionals, should under no circumstances rely upon this information as a substitute for their own research or for obtaining specific legal, accounting or tax advice from their own counsel. All information discussed herein is current only as of the date appearing in this material and is subject to change at any time without notice.

The information contained herein, including any information regarding specific investment products or strategies, is provided for informational and/or illustrative purposes only, and is not intended to be and should not be construed as an offer, solicitation or recommendation with respect to any investment transaction, product or strategy. Past performance is no guarantee of future results. All material has been obtained from sources believed to be reliable, but its accuracy, completeness and interpretation cannot be guaranteed.

Explore Specialized Advice

NorthernTrust.com

Careers

Office Locations

Contact Us

Legal/Privacy

Canada Accessibility

Cookie Preferences/Notice