Tips to Help Taxpayers Spot and Avoid Tax Scams

Email Phishing Scams

The IRS never initiates contact with taxpayers via email to request financial information. Instead, they mail a bill to the person who owes taxes or in certain situations they will call or visit your home or business.

Do not open any attachments, click links, reply to the sender, or take any actions that can put you at risk. To report suspicious online or email phishing scams, email phishing@irs.gov.

Phone Scams

The IRS and its authorized private collection agencies will not:

- Leave pre-recorded, urgent, or threatening messages on an answering system.
- Threaten to immediately bring in local police or other law enforcement groups to arrest the taxpayer.
- Call to demand immediate payment with a prepaid debit card, gift card, or wire transfer.
- Request checks to third parties.
- Demand payment without giving the taxpayer an opportunity to question or appeal the amount owed.

Be on the lookout for criminals who can fake or spoof caller ID numbers to appear to be from anywhere in the country. Furthermore, they can spoof an IRS office phone number or various local, state, federal, or tribal government agency numbers.

If you receive an IRS or Treasury-related phone call, but don't owe taxes and have no reason to believe you do, take the following actions:

1. Don't share any personal information and hang up.
2. Contact the Treasury Inspector General for Tax Administration to report the IRS impersonation scam call.
3. Report the caller ID and callback number to the IRS by sending it to phishing@irs.gov and include "IRS Phone Scam" in the subject line.
4. Report the call to the Federal Trade Commission.

If you stay vigilant against email and phone scams, you can rest assured that you are less likely to fall victim ton this fraudulent criminal activity.