

Be Alert to Scammers Who Pose as the IRS

Scammers pretending to be from the IRS continue to target taxpayers. These scams take many different forms. Among the most common are phone calls and fake emails. Thieves use the IRS name, logo or a fake website to try and steal money from taxpayers. Identity theft can also happen with such [scams](#).

Taxpayers need to be cautious of phone calls or automated messages from scammers who claim to be from the IRS. These criminals often say the taxpayer owes money. They also demand immediate payment. Scammers also lie to taxpayers and say they are due a refund. They do this to lure their victims into giving their bank account information over the phone. The IRS warns taxpayers not to fall for these scams.

Below are tips that will help avoid becoming a victim during the summer months and throughout the year:

The IRS will **NOT**:

- Call to demand immediate payment using specific payment method such as a prepaid debit card, gift card or wire transfer. Generally, the IRS first mails a bill to taxpayers who owe taxes. If the IRS assigns a case to a Private Debt Collector (PCA), both the IRS and the authorized collection agency send a letter to the taxpayer. Payment is always to the United States Treasury.
- Threaten to immediately bring in local police or other law-enforcement groups to have the taxpayer arrested for not paying.
- Demand payment of taxes without giving the taxpayer the opportunity to question or appeal the amount owed.
- Ask for credit or debit card numbers over the phone.

If a taxpayer does not owe any tax, they should:

- Contact the Treasury Inspector General for Tax Administration. Use TIGTA's "[IRS Impersonation Scam Reporting](#)" web page to report the incident.
- Report the incident to the Federal Trade Commission. Use the "[FTC Complaint Assistant](#)" on FTC.gov. Please add "IRS Telephone Scam" to the comments of your report.

If a taxpayer is not sure whether they owe any tax, they can [view their tax account](#) information on IRS.gov to find out.

Taxpayers should also watch out for emails and websites looking to steal personal information. An IRS phishing scam is an unsolicited, bogus email that claims to come from the IRS. Criminals often use fake refunds, phony tax bills or threats of an audit. Some emails link to fake websites that look real. The scammers' goal is to lure victims to give up their personal and financial information. If they're successful, they use it to steal a victim's money and their identity.

For taxpayers who get a ‘phishing’ email, the IRS offers this advice:

- Don’t reply to the message.
- Don’t give out personal or financial information.
- Forward the email to phishing@irs.gov. Then delete it.
- Do not open any attachments or click on any links. They may have malicious code that will infect your computer.

More information on how to [report phishing or phone scams](#) is available on [IRS.gov/phishing](https://www.irs.gov/phishing).

Avoid scams. The IRS does not initiate contact using social media or text message. The first contact normally comes in the mail. Those wondering if they owe money to the IRS can [view their tax account](#) information on IRS.gov to find out.

Additional IRS Resources:

- [Identity Protection Tips](#)
- [Identity Protection Home Page](#)
- [Publication 5027](#), Identity Theft Information for Taxpayers
- [Publication 5199](#), Tax Preparer Guide to Identity Theft
- [Publication 4524](#), Security Awareness-Identity Theft Flyer
- [Publication 4523](#), Beware of Phishing Schemes

IRS YouTube Videos:

- Tax Scams – [English](#) | [Spanish](#) | [ASL](#)
- Phishing-Malware – [English](#) | [Spanish](#) | [ASL](#)
- IRS ID Theft FAQ – Going After the Bad Guys – [English](#) | [Spanish](#) | [ASL](#)

Share this tip on social media -- #IRSTaxTip: Be Alert to Scammers Who Pose as the IRS.
<https://go.usa.gov/xRpTw>