Key Messages

Filing Season – February through April 2021

Data Protection and Identity Theft Prevention

This year, there's a heightened need for security as fraudsters seek to use COVID-19 to scare and scam people out of their identities or money. The IRS advocates for using the strongest security measures possible and to remain vigilant due to constantly evolving threats and scams from fraudsters.

One way people can protect themselves is to enroll in the IRS Identity Protection PIN program (IP PIN). It is an opt-in program available to all taxpayers who can verify their identities. An IP PIN is a six-digit code known only to the taxpayer and the IRS. It helps prevent identity thieves from filing fraudulent tax returns using a taxpayers' personally identifiable information. Electronic returns that do not have the correct IP PIN will be rejected, and paper returns will go through added scrutiny for fraud.

Note that the IRS does not:

- Demand that people use a specific payment method, such as a prepaid debit card, gift card or wire transfer. The IRS will not ask for debit or credit card numbers over the phone. People who owe taxes should make payments to the U.S. Treasury or review IRS.gov/payments for IRS online options.
- Demand immediate tax payment. Normal correspondence begins with a letter in the mail and taxpayers can appeal or question what they owe. All taxpayers are advised to know their rights as a taxpayer.
- Threaten to bring in local police, immigration officers or other law enforcement agencies to arrest people for not paying. The IRS also cannot revoke a license or immigration status. Threats like these are common tactics scam artists use to trick victims into believing their schemes.
- For more information on tax scams, please see Tax Scams/Consumer Alerts. For more information on phishing scams, please see Suspicious emails and Identity Theft.

Is it really the IRS?

- Criminals impersonate IRS employees and call taxpayers in aggressive and sophisticated ways. Imposters claim to be IRS employees and sound very convincing. They use fake names and phony IRS identification badge numbers. They're demanding and threatening – and do not reflect how the IRS handles enforcement matters.
- See Avoid scams: Know the facts on how the IRS contacts taxpayers for more information.
- Scammers send emails that trick businesses and taxpayers into thinking the messages are official communications from the IRS or others in the tax industry. As part of phishing schemes, scammers sometimes ask taxpayers about a wide range of topics, such as refunds and filing status. They might also ask taxpayers to confirm personal information, order transcripts and verify personal identification numbers.
- The IRS does not use email, text messages or social media to discuss tax debts or refunds with taxpayers.

How to report scams:

- Report impersonation scams to the Treasury Inspector General for Tax Administration at IRS Impersonation Scam Reporting.
- Report phone scams to the Federal Trade Commission using the FTC Complaint Assistant. Add "IRS Telephone Scam" in the notes.
- Report an unsolicited email claiming to be from the IRS or an IRS-related system like the Electronic Federal Tax Payment System to the IRS at phishing@irs.gov.

If taxpayers receive Form 1099-G for unemployment benefits they did not actually get because of identity theft, they should contact their appropriate state agency for a corrected form.