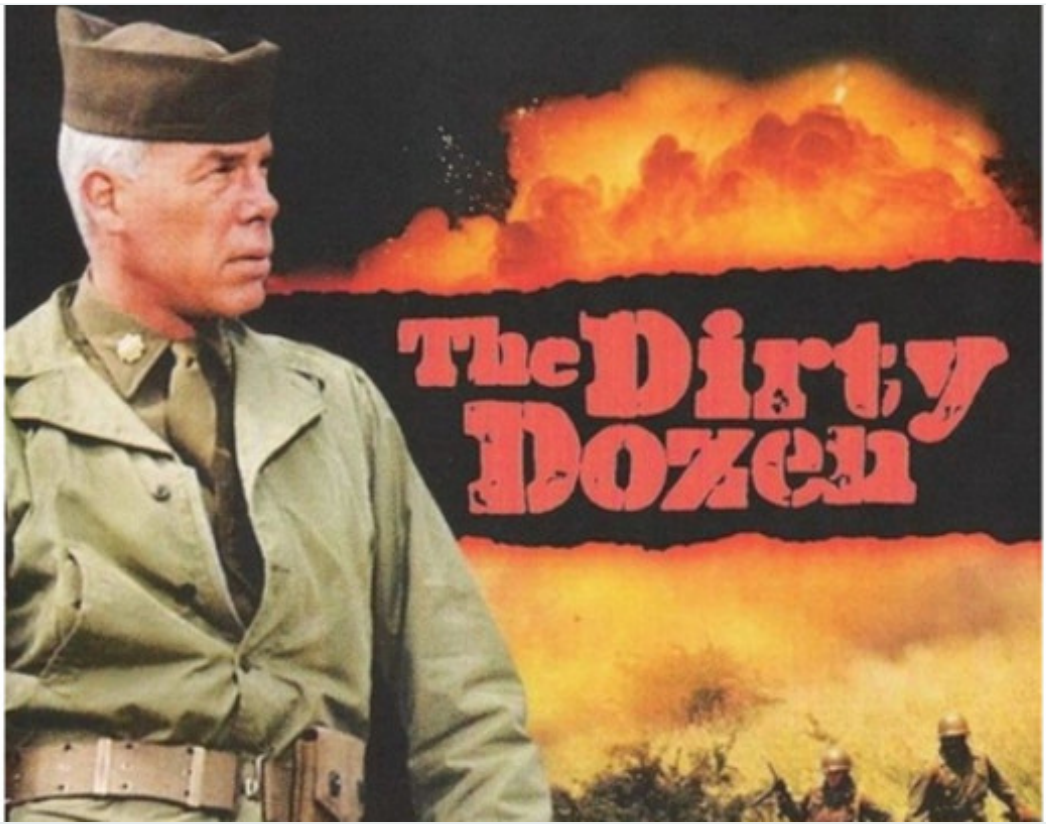
related scams like Economic Impact Payment theft; personal information cons including phishing, ransomware and phone 'vishing'; ruses focusing on unsuspecting victims ...

Jun. 29, 2021



The Internal Revenue Service has kicked off its "Dirty Dozen" list for 2021 with a warning for taxpayers, tax professionals and financial institutions to be on the lookout for these 12 nefarious schemes and scams.

This year's "Dirty Dozen" will be separated into four separate categories: **pandemic-related scams** like Economic Impact Payment theft; **personal information cons** including phishing, ransomware and phone 'vishing'; **ruses focusing on unsuspecting victims** like fake charities and senior/immigrant fraud; and **schemes**

that persuade taxpayers into unscrupulous actions such as Offer In Compromise

"We continue to see scam artists use the pandemic to steal money and information from honest taxpayers in a time of crisis," said IRS Commissioner Chuck Rettig. "We provide this list to alert taxpayers about common scams that fraudsters use against their victims. At the IRS, we are dedicated to stopping these criminals, but it's up to all of us to remain vigilant to protect ourselves and our families."

Taxpayers are encouraged to review the "Dirty Dozen: list in a special section on IRS.gov and should be alert to these scams during tax filing season and throughout the year.

Economic Impact Payment theft

A continuing threat to individuals is from identity thieves who try to steal Economic Impact Payments (EIPs), also known as stimulus payments. Most eligible people will get their payments automatically from the IRS. Taxpayers should watch out for these tell-tale signs of a scam:

- Any text messages, random incoming phone calls or emails inquiring about bank account information or requesting recipients to click a link or verify data should be considered suspicious and deleted without opening.
- Be alert to mailbox theft. Frequently check mail and report suspected mail losses to Postal Inspectors.
- Don't fall for stimulus check scams. The IRS won't initiate contact by phone, email, text or social media asking for Social Security numbers or other personal or financial information related to Economic Impact Payments.

Taxpayers should remember that the IRS website, IRS.gov, is the agency's official website for information on payments, refunds and other tax information.

Unemployment fraud leading to inaccurate taxpayer 1099-Gs

Because of the COVID-19 pandemic, many taxpayers lost their jobs and received

return, taxpayers should complete their return claiming only the unemployment compensation and other income they actually received. See Identity Theft and Unemployment Benefits for tax details and DOL.gov/fraud for state-by-state reporting information.

Additional protection to help protect taxpayers

IRS makes IP PINs available to all taxpayers – adding another layer of security

To help taxpayers avoid identity theft, the IRS this year made its Identity Protection PIN (IP PIN) program available to all taxpayers. Previously it was available only to victims of ID theft or taxpayers in certain states. The IP PIN is a six-digit code known only to the taxpayer and to the IRS. It helps prevent identity thieves from filing fraudulent tax returns using a taxpayer's personally identifiable information.

Using an IP PIN is, in essence, a way to lock a tax account. The IP PIN serves as the key to opening that account. Electronic returns that do not contain the correct IP PIN will be rejected and paper returns will go through additional scrutiny for fraud.

Reducing fraud

The IRS and its Security Summit partners in the states and the private-sector tax community have made changes to help reduce identity theft-related refund fraud that are noticeable to the average person filing a return:

- Tax software providers agreed to strengthen password protocols. This is the first line of defense for these companies to make sure their products are secure.
- State tax agencies began asking for taxpayers' driver's license numbers as another way for people to prove their identities.
- The IRS limited the number of tax refunds going to financial accounts or addresses.
- The IRS masked personal information from tax transcripts.

Multi-factor authentication can help

that allows them to quickly identify emerging scams and react to protect taxpayers. The Identity Theft Tax Refund Fraud Information Sharing and Analysis Center is now operational.

Also, check out our recent A *Closer Look* column for more on how to be vigilant about tax scams. Visit Identity Theft Central and Tax Fraud Alerts for more information on how to protect against or report identity theft or fraud.

Benefits • Income Tax • Taxes