IRS DIRTY DOZEN 12 TAX SCAMS THIS IS DIRECTLY FROM THE IRS WEBSITE

IRS YouTube Video:

- Dirty Dozen — English | Spanish | ASL

IR-2020-160, July 16, 2020

WASHINGTON — The Internal Revenue Service today announced its annual "Dirty Dozen" list of tax scams with a special emphasis on aggressive and evolving schemes related to coronavirus tax relief, including Economic Impact Payments.

This year, the Dirty Dozen focuses on scams that target taxpayers. The criminals behind these bogus schemes view everyone as potentially easy prey. The IRS urges everyone to be on guard all the time and look out for others in their lives.

"Tax scams tend to rise during tax season or during times of crisis, and scam artists are using pandemic to try stealing money and information from honest taxpayers," said IRS Commissioner Chuck Rettig. "The IRS provides the Dirty Dozen list to help raise awareness about common scams that fraudsters use to target people. We urge people to watch out for these scams. The IRS is doing its part to protect Americans. We will relentlessly pursue criminals trying to steal your money or sensitive personal financial information."

Taxpayers are encouraged to review the list in a special section on IRS.gov and be on the lookout for these scams throughout the year. Taxpayers should also remember that they are legally responsible for what is on their tax return even if it is prepared by someone else. Consumers can help protect themselves by choosing a reputable tax preparer.

The IRS urges taxpayers to refrain from engaging potential scammers online or on the phone. The IRS plans to unveil a similar list of enforcement and compliance priorities this year as well.

An upcoming series of press releases will emphasize the illegal schemes and techniques businesses and individuals use to avoid paying their lawful tax liability. Topics will include such scams as abusive micro captives and fraudulent conservation easements.

Here are this year's "Dirty Dozen" scams:

Phishing:

Taxpayers should be alert to potential fake emails or websites looking to steal personal information. The IRS will never initiate contact with taxpayers via email about a tax bill, refund or Economic Impact Payments. Don't click on links claiming to be from the IRS. Be wary of emails and websites − they may be nothing more than scams to steal personal information.

IRS Criminal Investigation has seen a tremendous increase in phishing schemes utilizing emails, letters, texts and links. These phishing schemes are using keywords such as "coronavirus," "COVID-19" and "Stimulus" in various ways.

These schemes are blasted to large numbers of people in an effort to get personal identifying information or financial account information, including account numbers and passwords. Most of these new schemes are actively playing on the fear and unknown of the virus and the stimulus payments. (For more see IR-2020-115, IRS warns against COVID-19 fraud; other financial schemes.)

Fake Charities:

Criminals frequently exploit natural disasters and other situations such as the current COVID-19 pandemic by setting up fake charities to steal from well-intentioned people trying to help in times of need. Fake charity scams generally rise during times like these.

Fraudulent schemes normally start with unsolicited contact by telephone, text, social media, e-mail or in-person using a variety of tactics. Bogus websites use names similar to legitimate charities to trick people to send money or provide personal financial information. They may even claim to be working for or on behalf of the IRS to help victims file casualty loss claims and get tax refunds.

Taxpayers should be particularly wary of charities with names like nationally known organizations. Legitimate charities will provide their Employer Identification Number (EIN), if requested, which can be used to verify their legitimacy. Taxpayers can find legitimate and qualified charities with the search tool on IRS.gov.

Threatening Impersonator Phone Calls:

IRS impersonation scams come in many forms. A common one remains bogus threatening phone calls from a criminal claiming to be with the IRS. The scammer attempts to instill fear and urgency in the potential victim. In fact, the IRS will never threaten a taxpayer or surprise him or her with a demand for immediate payment.

Phone scams or "vishing" (voice phishing) pose a major threat. Scam phone calls, including those threatening arrest, deportation or license revocation if the victim doesn't pay a bogus tax bill, are reported year-round. These calls often take the form of a "robocall" (a text-to-speech recorded message with instructions for returning the call).

The IRS will never demand immediate payment, threaten, ask for financial information over the phone, or call about an unexpected refund or Economic Impact Payment. Taxpayers should contact the real IRS if they worry about having a tax problem.

Social Media Scams:

Taxpayers need to protect themselves against social media scams, which frequently use events like COVID-19 to try tricking people. Social media enables anyone to share information with anyone else on the Internet. Scammers use that information as ammunition for a wide variety of scams. These include emails where scammers impersonate someone's family, friends or co-workers.

Social media scams have also led to tax-related identity theft. The basic element of social media scams is convincing a potential victim that he or she is dealing with a person close to them that they trust via email, text or social media messaging.

Using personal information, a scammer may email a potential victim and include a link to something of interest to the recipient which contains malware intended to commit more crimes. Scammers also infiltrate their victim's emails and cell phones to go after their friends and family with fake emails that appear to be real and text messages soliciting, for example, small donations to fake charities that are appealing to the victims.

EIP or Refund Theft:

The IRS has made great strides against refund fraud and theft in recent years, but they remain an ongoing threat. Criminals this year also turned their attention to stealing Economic Impact Payments as provided by the Coronavirus Aid, Relief, and Economic Security (CARES) Act.

Much of this stems from identity theft whereby criminals file false tax returns or supply other bogus information to the IRS to divert refunds to wrong addresses or bank accounts.

The IRS recently warned nursing homes and other care facilities that Economic Impact Payments generally belong to the recipients, not the organizations providing the care. This came following concerns that people and businesses may be taking advantage of vulnerable populations who received the payments. These payments do not count as a resource for determining eligibility for Medicaid and other federal programs They also do not count as income in determining eligibility for these programs. See IR-2020-121, IRS alert: Economic Impact Payments belong to recipient, not nursing homes or care facilities for more.

Taxpayers can consult the Coronavirus Tax Relief page of IRS.gov for assistance in getting their EIPs. Anyone who believes they may be a victim of identity theft should consult the Taxpayer Guide to Identity Theft on IRS.gov.

Senior Fraud:

Senior citizens and those who care about them need to be on alert for tax scams targeting older Americans. The IRS recognizes the pervasiveness of fraud targeting older Americans along with the Department of Justice and FBI, the Federal Trade Commission, the Consumer Financial Protection Bureau (CFPB), among others.

Seniors are more likely to be targeted and victimized by scammers than other segments of society. Financial abuse of seniors is a problem among personal and professional relationships. Anecdotal evidence across professional services indicates that elder fraud goes down substantially when the service provider knows a trusted friend or family member is taking an interest in the senior's affairs.

Older Americans are becoming more comfortable with evolving technologies, such as social media. Unfortunately, that gives scammers another means of taking advantage. Phishing scams linked to Covid-19 have been a major threat this filing season. Seniors need to be alert for a continuing surge of fake emails, text messages, websites and social media attempts to steal personal information.

Scams targeting non-English speakers:

IRS impersonators and other scammers also target groups with limited English proficiency. These scams are often threatening in nature. Some scams also target those potentially receiving an Economic Impact Payment and request personal or financial information from the taxpayer.

Phone scams pose a major threat to people with limited access to information, including individuals not entirely comfortable with the English language. These calls frequently take the form of a "robocall" (a text-to-speech recorded message with instructions for returning the call), but in some cases may be made by a real person. These con artists may have some of the

taxpayer's information, including their address, the last four digits of their Social Security number or other personal details – making the phone calls seem more legitimate.

A common one remains the IRS impersonation scam where a taxpayer receives a telephone call threatening jail time, deportation or revocation of a driver's license from someone claiming to be with the IRS. Taxpayers who are recent immigrants often are the most vulnerable and should ignore these threats and not engage the scammers.

Unscrupulous Return Preparers:

Selecting the right return preparer is important. They are entrusted with a taxpayer's sensitive personal data. Most tax professionals provide honest, high-quality service, but dishonest preparers pop up every filing season committing fraud, harming innocent taxpayers or talking taxpayers into doing illegal things they regret later.

Taxpayers should avoid so-called "ghost" preparers who expose their clients to potentially serious filing mistakes as well as possible tax fraud and risk of losing their refunds. With many tax professionals impacted by COVID-19 and their offices potentially closed, taxpayers should take particular care in selecting a credible tax preparer.

Ghost preparers don't sign the tax returns they prepare. They may print the tax return and tell the taxpayer to sign and mail it to the IRS. For e-filed returns, the ghost preparer will prepare but not digitally sign as the paid preparer. By law, anyone who is paid to prepare or assists in preparing federal tax returns must have a Preparer Tax Identification Number (PTIN). Paid preparers must sign and include their PTIN on returns.

Unscrupulous preparers may also target those without a filing requirement and may or may not be due a refund. They promise inflated refunds by claiming fake tax credits, including education credits, the Earned Income Tax Credit (EITC) and others. Taxpayers should avoid preparers who ask them to sign a blank return, promise a big refund before looking at the taxpayer's records or charge fees based on a percentage of the refund.

Taxpayers are ultimately responsible for the accuracy of their tax return, regardless of who prepares it. Taxpayers can go to a special page on IRS.gov for tips on choosing a preparer.

Offer in Compromise Mills:

Taxpayers need to wary of misleading tax debt resolution companies that can exaggerate chances to settle tax debts for "pennies on the dollar" through an Offer in Compromise (OIC). These offers are available for taxpayers who meet very specific

criteria under law to qualify for reducing their tax bill. But unscrupulous companies oversell the program to unqualified candidates so they can collect a hefty fee from taxpayers already struggling with debt.

These scams are commonly called OIC "mills," which cast a wide net for taxpayers, charge them pricey fees and churn out applications for a program they're unlikely to qualify for. Although the OIC program helps thousands of taxpayers each year reduce their tax debt, not everyone qualifies for an OIC. In Fiscal Year 2019, there were 54,000 OICs submitted to the IRS. The agency accepted 18,000 of them.

Individual taxpayers can use the free online Offer in Compromise Pre-Qualifier tool to see if they qualify. The simple tool allows taxpayers to confirm eligibility and provides an estimated offer amount. Taxpayers can apply for an OIC without third-party representation; but the IRS reminds taxpayers that if they need help, they should be cautious about whom they hire.

Fake Payments with Repayment Demands:

Criminals are always finding new ways to trick taxpayers into believing their scam including putting a bogus refund into the taxpayer's actual bank account. Here's how the scam works:

A con artist steals or obtains a taxpayer's personal data including Social Security number or Individual Taxpayer Identification Number (ITIN) and bank account information. The scammer files a bogus tax return and has the refund deposited into the taxpayer's checking or savings account. Once the direct deposit hits the taxpayer's bank account, the fraudster places a call to them, posing as an IRS employee. The taxpayer is told that there's been an error and that the IRS needs the money returned immediately or penalties and interest will result. The taxpayer is told to buy specific gift cards for the amount of the refund.

The IRS will never demand payment by a specific method. There are many payment options available to taxpayers and there's also a process through which taxpayers have the right to question the amount of tax we say they owe. Anytime a taxpayer receives an unexpected refund and a call from us out of the blue demanding a refund repayment, they should reach out to their banking institution and to the IRS.

Payroll and HR Scams:

Tax professionals, employers and taxpayers need to be on guard against phishing designed to steal Form W-2s and other tax information. These are Business Email Compromise (BEC) or Business Email Spoofing (BES). This is particularly true with many businesses closed and their employees working from home due to COVID-19. Currently, two of the most common types of these scams are the gift card scam and the direct deposit scam.

In the gift card scam, a compromised email account is often used to send a request to purchase gift cards in various denominations. In the direct deposit scheme, the fraudster may have access to the victim's email account (also known as an email account compromise or "EAC"). They may also impersonate the potential victim to have the organization change the employee's direct deposit information to reroute their deposit to an account the fraudster controls.

BEC/BES scams have used a variety of ploys to include requests for wire transfers, payment of fake invoices as well as others. In recent years, the IRS has observed variations of these scams where fake IRS documents are used in to lend legitimacy to the bogus request. For example, a fraudster may attempt a fake invoice scheme and use what appears to be a legitimate IRS document to help convince the victim.

The Direct Deposit and other BEC/BES variations should be forwarded to the Federal Bureau of Investigation Internet Crime Complaint Center (IC3) where a complaint can be filed. The IRS requests that Form W-2 scams be reported to: phishing@irs.gov (Subject: W-2 Scam).

Ransomware:

This is a growing cybercrime. Ransomware is malware targeting human and technical weaknesses to infect a potential victim's computer, network or server. Malware is a form of invasive software that is often frequently inadvertently downloaded by the user. Once downloaded, it tracks keystrokes and other computer activity. Once infected, ransomware looks for and locks critical or sensitive data with its own encryption. In some cases, entire computer networks can be adversely impacted.

Victims generally aren't aware of the attack until they try to access their data, or they receive a ransom request in the form of a pop-up window. These criminals don't want to be traced so they frequently use anonymous messaging platforms and demand payment in virtual currency such as Bitcoin.

Cybercriminals might use a phishing email to trick a potential victim into opening a link or attachment containing the ransomware. These may include email solicitations to support a fake COVID-19 charity. Cybercriminals also look for system vulnerabilities where human error is not needed to deliver their malware.

The IRS and its Security Summit partners have advised tax professionals and taxpayers to use the free, multi-factor authentication feature being offered on tax preparation software products. Use of the multi-factor authentication feature is a free and easy way to protect clients and practitioners' offices from data thefts. Tax software providers also offer free multi-factor authentication protections on their Do-It-Yourself products for taxpayers.

Page Last Reviewed or Updated: 20-Jul-2020