IRS Dirty Dozen Scam List: Don't Be a Victim

IRS YouTube Video:

July 16, 2020 - Dirty Dozen — English | Spanish | ASL

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 . . .

1. **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.
2. **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.

ISBDC@LCSC.edu 208-792-2465 IdahoSBDC.org

3. **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.
4. **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.
5. **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.
6. **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.
7. **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.

8. **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 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.
9. **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.
10. **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.

11. **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. 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).

12. **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.

For complete list go to irs.gov/newsroom/irs-unveils-dirty-dozen-list-of-tax-scams-for-2020-americans-urged-to-be-vigilant-to-these-threats-during-the-pandemic-and-its-aftermath

ISBDC@LCSC.edu 208-792-2465 IdahoSBDC.org