Tax Scams of 2020

July 22, 2020

In an Information Release, the IRS has announced its annual “dirty dozen” tax scams for 2020.

Background. Every year, the IRS compiles a list of common tax scams (the “dirty dozen”) that taxpayers may encounter during the year. (via IRS. gov)

"Dirty dozen" scams list for 2020. This year, the “dirty dozen” list focuses on scams that target individual taxpayers, with special emphasis on aggressive and evolving schemes related to COVID-19 tax relief, including Economic Impact Payments (EIPs). The IRS urges taxpayers and tax professionals to be aware of these scams and not to engage with potential scammers online or on the phone.

This year’s "dirty dozen" scams list includes:

Phishing scams. According to the Information Release, 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 (EIP).

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

Fake charities. According to the Information Release, criminals frequently exploit natural disasters and other situations, such as the current COVID-19 pandemic, by setting up fake charities to steal from people trying to help in times of need. 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 those of 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 that mimic those of nationally known organizations.

Threatening IRS impersonator phone calls. According to the Information Release, IRS impersonation scams come in many forms but a common scam is bogus threatening phone calls from a criminal claiming to be with the IRS.

The Information Release notes that the IRS will never threaten a taxpayer or demand immediate payment, ask for financial information over the phone, or call about an unexpected refund or Economic Impact Payment (EIP).

Social media scams. According to the Information Release, 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 and scammers use that information for a wide variety of scams.

EIP or refund theft. According to the Information Release, in addition to stealing tax refunds, this year criminals turned their attention to stealing EIPs. EIPs are one-time payments to taxpayers provided by the Coronavirus Aid, Relief, and Economic Security (CARES) Act. Criminals use stolen information to file false tax returns or supply other bogus information to the IRS to divert refunds to wrong addresses or bank accounts.

The IRS recommends that taxpayers who need assistance getting an EIP consult the Coronavirus Tax Relief page. And taxpayers who believe they may be a victim of identity theft should consult the Taxpayer Guide to Identity Theft.

Senior fraud. According to the Information Release, senior citizens and those who care about them need to be on alert for tax scams targeting older Americans. Seniors are more likely to be targeted and victimized by scammers than other segments of society. Older Americans' increasing engagement with social media gives scammers another way to engage with seniors.

The IRS warns seniors 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. According to the Information Release, IRS impersonators and other scammers target groups with limited English proficiency. These scams are often threatening in nature. A common IRS impersonation scam involves a taxpayer receiving 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.

The IRS recommends that taxpayers who receive these types of phone calls should ignore the threats and not engage with the scammers.

"Ghost" and other bad return preparers. According to the Information Release, "ghost" return preparers don't sign the tax returns they prepare. They may print the prepared tax return and tell the taxpayer to sign it and mail it to the IRS or not digitally sign an efiled return as a paid preparer. By law, paid preparers must sign and include their Preparer Tax Identification Number (PTIN) on returns.

The Information Release also warns taxpayers to beware of preparers who promise inflated refunds by claiming fake tax credits, who ask the taxpayer 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.

The IRS has tips on how to choose a tax preparer that can be found here.

Tax debt resolution companies. The Information Release cautions taxpayers to beware of tax debt resolution companies that exaggerate their ability to settle tax debts for "pennies on the dollar" through an offer in compromise (OIC).

An OIC allows a taxpayer to settle a tax debt for less than the full amount owed; it may be a legitimate option if the taxpayer can't pay the full tax liability or doing so creates a financial hardship. (IRS.gov)

However, as the IRS notes in the Information Release, to qualify for an OIC, taxpayers must meet very specific criteria. The Information Release recommends that taxpayers use the IRS's free online Offer in Compromise Pre-Qualifier tool to see if they qualify for an offer-in-compromise, and obtain an estimated offer amount, without paying fees to a debt resolution company. Taxpayers can also apply for an OIC without third-party representation but, if they need help, the Information Release recommends that taxpayers be careful about whom they hire.

Fake payments with repayment demands. According to the Information Release, 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: 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 scammer calls the taxpayer posing as an IRS employee and asks the taxpayer to return the money via a specific type of gift cards for the amount of the refund.

The Information Release states that 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. The Information Release recommends that 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. The Information Release warns tax professionals, employers and taxpayers to be on guard against phishing designed to steal Form W-2s and other tax information, particularly now with many businesses closed and their employees working from home due to COVID-19.

These are Business Email Compromise (BEC) or Business Email Spoofing (BES) scams. 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 and impersonate the potential victim to change the victim'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.

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).

In the Information Release, the IRS requests that Form W-2 scams be reported to: phishing@irs.gov (Subject: W-2 Scam).

Ransomware. Ransomware is malware that, once downloaded, looks for and locks critical or sensitive data on the victim's computer with its own encryption. In some cases, entire computer networks can be adversely impacted. Scammers may use a phishing email to trick a potential victim into opening a link or attachment containing the ransomware. These email may include solicitations to support a fake COVID-19 charity or allegedly contain information about Economic Impact Payments.

The Information Release recommends that taxpayers and tax professionals use the free, multi-factor authentication feature available with their tax preparation software to protect against data thefts.

The IRS has previously said that multi-factor authentication means returning users must enter their username/password credentials plus another data point that only they know, such as a security code sent to their mobile phone.