JEFFREY S. ROSELL
DISTRICT ATTORNEY

**OFFICE OF
THE DISTRICT ATTORNEY**

COUNTY OF SANTA CRUZ

Santa Cruz
701 Ocean Street, Room 200
Santa Cruz, CA 95060
(831) 454-2400
dao@co.santa-cruz.ca.us

Website
http://datinternet.co.santa-cruz.ca.us/

FOR IMMEDIATE RELEASE
August 18, 2020

Contact: Doug Allen (831) 454-2400

DISTRICT ATTORNEY'S OFFICE WARNS OF IRS TAX SCAMS

2020 IRS List of Dirty Dozen Tax Scams

Not surprisingly, the 2020 list is loaded with coronavirus-related scams. Don't be a victim of the Dirty Dozen! Stay alert and stay safe. Be on the lookout for these Dirty Dozen scams of 2020:

1. **Phishing**: Fake emails or websites impersonate the IRS in an attempt to steal information about refunds or Economic Impact Payments (EIPs).

   Protect yourself: The IRS will never initiate contact with taxpayers via email. Be extra wary of any websites and emails making heavy use of COVID-19 terms like stimulus, coronavirus, and Economic Impact Payment.

2. **Fake charities**: Criminals exploit the fear and uncertainty surrounding the pandemic to set up bogus charities that rob innocent victims who believe they are helping the unfortunate. The "charity" may even claim to be working on behalf of the IRS to help victims of the virus get their tax refunds.

   Protect yourself: Charities with familiar-sounding names that aggressively market themselves are often bogus charities trying to make donors believe they represent the actual well-known organization. They will also refuse to provide an Employer Identification Number (EIN) when asked, and will not have a positive review on sites like Charity.org. Taxpayers can also search for legitimate charities using the IRS charity search tool.

3. **Threatening impersonator phone calls**: An alleged IRS agent threatens the victim with arrest, deportation, or license revocation if taxes are not paid immediately by prepaid gift card or wire transfer.

   Protect yourself: The IRS will never threaten a taxpayer or demand immediate payment over the phone. It also will not insist on being paid via gift card or wire transfer.

4. **Social media scams**: Scammers use information that can be found on social media platforms for a variety of scams, including the impersonation of friends to get at the victims' more private information. This ruse often ends in tax-related identity theft.

   Protect yourself: The "friend" will claim to be in a compromised position and to urgently need the victim's personal information. When contacted privately, though, the actual friend will have no knowledge of the interaction.

5. **EIP or refund theft**: Scammers steal taxpayers' identities, file false tax returns in their names, and pocket their refunds and their EIPs.

   Protect yourself: Personal information should never be shared online with an unverified contact, even if the contact promises to assist in tax filing or receiving the EIP.

6. **Senior fraud**: Scammers, or long-term caregivers of the elderly, file tax returns on their behalf and then pocket the refunds and EIPs.

   Protect yourself: Seniors should be wary of bogus emails, text messages, and fake websites asking them to share their personal information.

7. **Scams targeting non-English speakers**: Scammers impersonate IRS agents and target non-English speakers, threatening jail time, deportation, or revocation of the victim's driver's license if an immediate tax payment is not made. The victims have limited access to information and often fall for these scams.

   Protect yourself: The IRS will not threaten taxpayers over the phone or insist upon immediate payment.

8. **Unscrupulous return preparers**: Alleged tax preparers will reach out to the victim and offer their services. Unfortunately, though, they will steal the victim's personal information, file a tax return on their behalf, and pocket the refund, or promise inflated refunds for a bigger fee.

   Protect yourself: If a tax preparer is not willing to share their preparer Tax Identification Number (TIN), they are likely a scammer. Also, if the alleged preparer promises credits and deductions that sound too good to be true, they probably are.

9. **Offer in Compromise scams**: Bogus tax debt resolution companies make false claims about settling tax debts for "pennies on the dollar" through an Offer in Compromise (OIC) in exchange for a steep fee.

   Protect yourself: An OIC that sounds outrageously attractive is likely bogus. Taxpayers can use the IRS's OIC tool to see if they qualify for an authentic offer.

10. **Fake payments with repayment demands**: A scammer steals a taxpayer's personal information, files a fake tax return on their behalf, and has the refund deposited into the taxpayer's checking account. The scammer then calls the victim impersonating the IRS and claiming the refund was mistakenly inflated, so the victim must return the extra funds via gift card or wire transfer. Of course, this money will go directly into the scammers' pockets.

    Protect yourself: Refund checks will never be deposited in a taxpayer's account if they have not filed taxes. Also, the IRS does not demand payment by a specific method.

11. **Payroll and HR scams**: Scams target tax professionals, employers, and taxpayers to steal W-2s and other tax information. They will then impersonate the employee and request to change their direct deposit information for their paychecks.

    Protect yourself: If an employer or HR representative receives a request for a direct deposit change, it is best to check with the employee directly to see if the request is legitimate.

12. **Ransomware**: Malware infects a victim's computer, network, or server, and tracks keystrokes and/or other computer activity. Sensitive data is then encrypted and locked. When the victim tries to access their data, they will receive a pop-up message demanding a ransom payment for the return of their information.

    Protect yourself: Links embedded in emails from unverified sources should never be opened. Tax software should not be downloaded unless it features multi-factor authentication.

Are you or someone you know a victim of a scam? Contact your local law enforcement agency and file a report, file a complaint with the Federal Trade Commission (FTC) online, or file an online complaint with the Consumer Unit of the Santa Cruz County District Attorney's Office.