**BizBoost News  
Volume 12, Issue 7  
For distribution 10/03/22; publication 10/06/22**

**The “Dirty Dozen” IRS Tax Scams for 2022**

Each year, the IRS unveils its list of scams that target unsuspecting taxpayers. Below are five of the most common tax scams impacting taxpayers today, as well as tips to not become a victim:

1. **Pandemic-related scams.** Criminals still use the COVID-19 pandemic to steal people's money and identity with phishing emails, social media posts, phone calls, and text messages. These actions can lead to sensitive personal information being stolen, which scammers will use to harm victims in multiple ways, including trying to file a fraudulent tax return. Some of the scams people should continue to be on the lookout for include Economic Impact Payment and tax refund scams, unemployment fraud, fake employment offers on social media, and bogus charities that steal taxpayers' money. [Read more](about:blank) at <https://www.irs.gov/newsroom/irs-continues-with-dirty-dozen-this-week-urging-taxpayers-to-continue-watching-out-for-pandemic-related-scams-including-theft-of-benefits-and-bogus-social-media-posts> on pandemic-related scams.
2. **Offer in Compromise “mills.”** If you owe the IRS a substantial amount of money that you are having trouble paying, you could fall victim to marketing claims of Offer in Compromise (OIC) "mills." An Offer in Compromise is a real IRS term for an agreement between the taxpayer and the IRS that creates a payment plan based on the taxpayer’s situation. The mills make ridiculous claims about how they can settle a person's tax debt for pennies on the dollar. The reality is that taxpayers pay the OIC mill a fee to get the same deal they could have gotten themselves by working directly with the IRS. These "mills" tend to be especially visible right after the filing season ends and taxpayers are trying to resolve their tax issues, perhaps after receiving a balance due notice in the mail, but they remain a problem all year long. [Read more](about:blank) at <https://www.irs.gov/newsroom/dirty-dozen-irs-urges-anyone-having-trouble-paying-their-taxes-to-avoid-anyone-claiming-they-can-settle-tax-debt-for-pennies-on-the-dollar-known-as-oic-mills> on Offer in Compliance “mills”.
3. **Potentially abusive arrangements.** This group comprises of four types of transactions that are wrongfully promoted and likely to trigger an IRS audit in the future. These include using charitable remainder annuity trusts to eliminate taxable gains, contributing to Maltese (or other foreign) individual retirement arrangements, participating in foreign captive insurance arrangements, and using monetized installment sales. [Read more](about:blank) at <https://www.irs.gov/newsroom/irs-warns-taxpayers-of-dirty-dozen-tax-scams-for-2022> on these particular abusive arrangements.
4. **Suspicious Communication.** These forms of communication are designed to trick, surprise, or scare someone into responding before thinking. The IRS warns taxpayers to be on the lookout for suspicious activity across four common types of communication: email, social media, telephone, and text messages. Criminals use these bogus communications to trick victims into providing sensitive personal financial data, money, or other information. This information can be used to file false tax returns, access financial accounts, or for other schemes. [Read more](about:blank) at <https://www.irs.gov/newsroom/dirty-dozen-scammers-use-every-trick-in-their-communication-arsenal-to-steal-your-identity-personal-financial-information-money-and-more> on suspicious communication.
5. [**Spear Phishing Attacks**](about:blank)**.** Spear phishing is an email scam where criminals try to steal client data and tax preparers' identities to file fraudulent tax returns for refunds. Spear phishing can be directed towards any type of business or organization, so everyone needs to be on high alert and skeptical of strange emails requesting financial or personal information. For example, a recent spear phishing email used the IRS logo and a variety of subject lines such as "Action Required: Your account has now been put on hold" to steal tax professionals' software preparation credentials. The scam email will direct users to a website that shows the logos of several popular tax software preparation providers, and clicking on one of these logos will prompt a request for tax preparer account credentials. The IRS has observed similar spear phishing emails claiming to be from "tax preparation application providers." Tax pros and taxpayers should not respond or take any of the steps outlined in any such questionable emails. [Read more](about:blank) at https://www.irs.gov/newsroom/dirty-dozen-irs-security-summit-reiterate-recent-warning-to-tax-professionals-and-other-businesses-of-dangerous-spear-phishing-attacks on spear phishing scams.

Please take care to protect your personal financial information. For more on the [IRS Dirty Dozen List](about:blank), visit <https://www.irs.gov/newsroom/dirty-dozen> on the IRS website.

\*\*\*

Tweets

Insert a link to your newsletter, website or blog before you post these:

Our latest blog: “The “Dirty Dozen” IRS Tax Scams for 2022” is available now! Subscribe here: [link]

Each year, the IRS unveils its list of scams that target unsuspecting taxpayers. Learn about the five most common tax scams impacting taxpayers today in our latest blog article: [link]

Criminals still use the COVID-19 pandemic to steal people's money and identity with phishing emails, social media posts, phone calls, and text messages. These actions can lead to sensitive personal information being stolen, which scammers will use to harm victims in multiple ways, including trying to file a fraudulent tax return. Learn more in our latest blog article: [link]

Suspicious forms of communication are designed to trick, surprise, or scare someone into responding before thinking. The IRS warns taxpayers to be on the lookout for suspicious activity across four common types of communication: email, social media, telephone, and text messages. Learn more here: [link]

If you owe the IRS a substantial amount of money that you are having trouble paying, you could fall victim to marketing claims of Offer in Compromise (OIC) "mills." An Offer in Compromise is a real IRS term for an agreement between the taxpayer and the IRS that creates a payment plan based on the taxpayer’s situation. Find out more here: [link]

Spear phishing is an email scam where criminals try to steal client data and tax preparers' identities to file fraudulent tax returns for refunds. Spear phishing can be directed towards any type of business or organization, so everyone needs to be on high alert and skeptical of strange emails requesting financial or personal information. Learn more here: [link]

There are four types of transactions that are wrongfully promoted and likely to trigger an IRS audit in the future. Learn what these transactions are in our latest blog article: [link]

Do you know the five most common tax scams impacting taxpayers? Sign up for our newsletter to learn what they are and how to increase your awareness of them: [link]