BCLP. Client Intelligent

BCLPCharityLaw.com

ACCESSING IRS ONLINE SERVICES UNDERSTANDING THE IDENTITY VERIFICATION PROCESS

Jul 15, 2022

The IRS is presenting a live webinar offering 1 continuing education credit, discussing:

- Improved access to IRS online services
- What this means for e-Services users
- IRS's new identity verification and authentication platform
- Registration overview
- Key takeaways
- Plus, a live Q&A

When: Tuesday, July 19, 2022 @ 2:00 pm Eastern

IRS warns taxpayers of "Dirty Dozen" tax scams for 2022

Compiled annually, the Dirty Dozen lists a variety of common scams that taxpayers can encounter anytime. The IRS warns taxpayers, tax professionals and financial institutions to beware of these scams. This year's Dirty Dozen list is divided into five groups.

Potentially abusive arrangements - The 2022 Dirty Dozen begins with four abusive transactions that are wrongfully promoted and will likely attract additional IRS compliance efforts in the future.

- charitable remainder annuity trusts,
- Maltese individual retirement arrangements,
- foreign captive insurance, and
- monetized installment sales.

Pandemic-related scams - This IRS reminds taxpayers that 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. Be on the lookout for

- Economic Impact Payment and tax refund scams,
- unemployment fraud leading to inaccurate taxpayer 1099-Gs,
- fake employment offers on social media, and
- fake charities that steal taxpayers' money.

Offer in Compromise "mills" - Offer in Compromise or OIC "mills," make outlandish claims, usually in local advertising, about how they can settle a person's tax debt for pennies on the dollar. Often, the reality is that taxpayers pay the OIC mill a fee to get the same deal they could have gotten on their own by working directly with the IRS.

Suspicious communications - Every form of suspicious communication is designed to trick, surprise, or scare someone into responding before thinking. Criminals use a variety of communications to trick victims into providing personal information that can be used to file false tax returns and tap into financial accounts. lure potential victims. You should lookout for suspicious communications via email, social media, telephone and text messages.

Spear phishing attacks - Spear phishing scams target individuals or groups. Criminals try to steal client data and tax preparers' identities to file fraudulent tax returns for refunds. Spear phishing can be tailored to attack any type of business or organization, so everyone needs to be skeptical of emails requesting financial or personal information.

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.

RELATED PRACTICE AREAS

- Non Profit Organizations
