

IRS News Release

Media Relations Office

Washington, D.C.

Media Contact: 202.317.4000

www.irs.gov/newsroom

Public Contact: 800.829.1040

Identity Theft Remains on “Dirty Dozen” List of Tax Scams; IRS, States, Tax Industry Urge People to be Vigilant Against Criminals

IRS YouTube Videos:

Security Summit: Check your Credit Report Annually – [English](#)

Security Summit: Secure Your Tax Return – [English](#)

Security Summit: Be Careful When Using Wi-Fi – [English](#)

Security Summit: Update Your Password Regularly – [English](#)

Taxes.Security.Together. – [English](#)

Protect Your Clients; Protect Yourself - [English](#)

Dirty Dozen – [English](#) | [Spanish](#) | [ASL](#)

IR-2017-22, Feb. 3, 2017

WASHINGTON — The Internal Revenue Service today issued a filing season alert, warning taxpayers and tax professionals to watch out for identity theft at tax time, and highlighted the crime as a recurring scam in the agency’s [“Dirty Dozen”](#) series.

The Dirty Dozen is compiled annually by the IRS and lists a variety of common scams taxpayers may encounter any time during the year. Many of these con games peak during filing season as people prepare their tax returns or hire tax professionals.

Tax-related Identity theft – with its related scams to steal personal and financial data from taxpayers or data held by tax professionals – remains a top item on the Dirty Dozen list. It remains an ongoing concern even though progress is being made.

The IRS, state tax agencies and the tax industry have joined as the Security Summit and enacted a series of safeguards that are showing results. In 2016, the number of taxpayers reporting stolen identities on federal tax returns fell by more than 50 percent, with nearly 275,000 fewer victims compared to a year ago.

To further these efforts, the [Security Summit](#) partners applied more safeguards in 2017 and continue to seek new and expanded ways to reduce identity theft. Because of these successes, criminals are devising more creative ways to steal personal information and impersonate taxpayers.

“The Security Summit partnership continues to develop and strengthen tools to stop fraudulent returns from getting into the tax system,” said IRS Commissioner John Koskinen. “We’re calling on taxpayers to do everything they can to protect their private information because criminals continue looking for new and more sophisticated ways of beating the system. We also encourage tax professionals and others in the private and non-profit sectors with access to large amounts of sensitive information to watch out for identity theft schemes.”

Security Reminders for Taxpayers

The IRS and its partners remind taxpayers they can do their part to help in this effort. Taxpayers and tax professionals should:

- Always use security software with firewall and anti-virus protections. Make sure the security software is always turned on and can automatically update. Encrypt sensitive files such as tax records stored on the computer. Use strong passwords.
- Learn to recognize and avoid phishing emails, threatening phone calls and texts from thieves posing as legitimate organizations such as banks, credit card companies and government organizations, including the IRS. Do not click on links or download attachments from unknown or suspicious emails.
- Protect personal data. Don't routinely carry a Social Security card, and make sure tax records are secure. Treat personal information like cash; don't leave it lying around.

"Everyone should guard their personal information by protecting their computers and using extreme caution when viewing emails or getting surprise phone calls," Koskinen said. "We also encourage people to share this information with their friends and family. We all know someone who is challenged by technology, and some easy, common-sense steps could help protect these people from identity theft."

The Security Summit launched a "[Taxes. Security. Together.](#)" public awareness campaign aimed at taxpayers. This campaign provided easy tips to taxpayers to protect themselves, including video, tax tips and fact sheets to stay safe online. The Summit also initiated a "[Protect Your Clients; Protect Yourself](#)" campaign aimed at tax professionals who are increasingly targeted by cybercriminals.

Tax-related identity theft occurs when someone uses a stolen Social Security number or Individual Taxpayer Identification Number (ITIN) to file a tax return claiming a fraudulent refund.

The IRS understands that undoing the damage caused by identity theft is a frustrating and complex process for victims. While identity thieves steal information from sources outside the tax system, the IRS is often the first to inform a victim that identity theft has occurred. The IRS is working hard to resolve identity theft cases as quickly as possible. For more information, see the special [identity theft section on IRS.gov](#).

Related Items:

- [IR-2016-144](#), IRS, Security Summit Partners Expand Identity Theft Safeguards for 2017 Filing Season, Build on 2016 Successes
- [FS-2015-23](#), IRS, States and Industry Partners Provide Update on Collaborative Fight Against Tax-Related Identity Theft
- [IRS Tax Tip](#): IRS, Partners Add New Safeguard for 2017; Ask for Your Help to Combat Identity Theft