



News Release

Media Relations Office

Washington, D.C.

Media Contact: 202.317.4000

www.IRS.gov/newsroom

Public Contact: 800.829.1040

IRS, States and Tax Industry Announce New Steps to Help Public to Protect Personal Tax Data**IRS YouTube Video:***Taxes. Security. Together.* – [English](#)

IR-2015-129, Nov. 19, 2015

WASHINGTON — The Internal Revenue Service, state tax administrators and the private-sector tax industry today announced a new campaign aimed at encouraging more people to protect their personal and financial data online and at home.

The “Taxes. Security. Together.” campaign is designed to raise public awareness that even routine actions on the Internet and their personal devices can affect the safety of their financial and tax data. The education campaign will complement the expanded series of protections the IRS, states and tax industry are putting in place for the start of the 2016 filing season to address tax-related identity theft. (See [IR-2015-117](#) and [Fact Sheet 2015-23](#).)

“Identity thieves are evolving, and so must we. Everyone has a part to play,” said IRS Commissioner John Koskinen. “The IRS, the states and the tax industry are putting in place even tougher safeguards for 2016. But, we need the public’s help. We need people to join with us and take an active role in protecting their personal and financial data from thieves.”

The campaign -- which will continue through the April tax deadline -- was announced today at an event hosted by the Federation of Tax Administrators, comprised of state revenue departments across the nation. The effort is part of the Security Summit, a collaborative effort started in March between the states, the IRS and the tax industry.

The joint consumer campaign includes several components, including YouTube videos, consumer-friendly Tax Tips each week and local events across the country. Several IRS publications have been added or updated to help taxpayers and tax professionals. The information will also be shared across IRS.gov, state web sites and platforms used by the tax software community and others in the tax community.

“The governments and industry are taking new steps to protect taxpayers. To build on this even further, we are joining forces to share important information across our websites - whether it's at the state level, in the tax industry or at the IRS. This is an unprecedented collaborative effort for tax administration,” said David Sullivan, Tax Administrator for the

Rhode Island Division of Taxation and immediate past president of the Federation of Tax Administrators.

It is clear that increasingly sophisticated identity thieves have access to excessive amounts of personal and financial data, which they buy and sell on the black market, and use this data to file fraudulent tax returns using victims' names and Social Security numbers. While the IRS, states and tax industry are taking new steps to toughen their systems to protect taxpayers, there are also things people can do as well.

"People handle some of their most sensitive personal and financial information when they prepare their taxes on their home computer. But when they sit down, we want to help make sure they are preparing their taxes on a device that is secure. Tax time is two months away, but it's not too early for people to make sure they are doing the right things to protect themselves," said Bernie McKay, an executive vice president at Intuit, one of more than 20 members of the tax industry participating in the Summit process.

The IRS, states and tax industry are urging the public to take active steps to protect themselves. The partners are encouraging people to:

- **Use security software to protect computers.** This includes a firewall and anti-virus protection. If tax returns or sensitive data are stored on the computers, encrypt the files. Use strong passwords.
- **Beware of phishing emails and phone scams.** A common way for identity thieves to steal names and Social Security numbers, passwords, credit card numbers, bank account information is to simply ask for it. Clever criminals pose as trusted organizations that you recognize and send spam emails, calls or texts. Their email may ask you to update a bank account or tax software account and provide a link that to a fake website that is designed solely to steal your logon information. They may call posing as the IRS threatening you with jail or lawsuits unless you make an immediate payment. They may provide an attachment which, if you download, will infect your machine and enable the thief to access sensitive files or track your key strokes.
- **Protect personal information.** Do not routinely carry your Social Security number. Properly dispose of old tax returns and other sensitive documents by shredding before trashing. Check your credit reports and Social Security Administration accounts at least annually to ensure no one is using your good credit or using your SSN for employment. Oversharing on social media also gives identity thieves even more personal details.

"These are all basic, common sense steps that you no doubt have heard many times if you are a regular Internet user. But there are 150 million households that file taxes, and problems still happen. Security software still gets turned off. And there are still, on a regular basis, victims who are tricked by these clever phishing schemes. Not only can this

harm the individuals attacked, this can have a direct impact on tax administration," Koskinen said.

The partners are asking all tax preparers and businesses to share information with employees, clients and customers. See www.irs.gov/taxesecuritytogether for more information. There also is [IRS Publication 4524, Security Awareness for Taxpayers](#), which provides a brief overview of steps people can take.

In March, Koskinen convened an unprecedented meeting of IRS, state tax officials and the tax industry to determine what additional steps could be taken. On October 20, the Security Summit participants provided an update to the public.

For the 2016 filing season, there will be new standards for logging onto all tax software products such as minimum password requirements, new security questions and standard lockout features. The software industry will provide more than 20 additional data elements from the tax return submission to the IRS and, in turn, to the states to help identify fraudulent returns. All parties agreed to information sharing on a weekly basis to help quickly identify and adjust to new and emerging tax-related fraud schemes.

The IRS also continues to work to help victims of identity theft and pursue criminals using identity information to file fraudulent tax returns. IRS Criminal Investigation has worked on thousands of identity theft cases. Since 2013, nearly 2,000 identity thieves have been convicted, with the average sentence running well over three years.