A Security Summit 2020 Filing Season Identity Theft Initiative

NATIONAL TAX SECURITY AWARENESS WEEK PARTNER TOOLKIT

Dec. 2-Dec. 6 2019

2020 Filing Season

Ready-to-Use (copy and paste) communication products such as news conference script/talking points, generic news release, articles/ emails and suggested multilingual social media posts. IRS News Releases also available in English and Spanish. All material can be used and shared by partner groups during the awareness week or throughout the 2020 filing season.

Publication 5372 (10-2019) Catalog Number 73426M Department of the Treasury **Internal Revenue Service** www.irs.gov

Table of Contents

Welcome to National Tax Security Awareness Week 2019 (December 2 through December 6)

Anchored between the holiday shopping season and the upcoming tax filing season, National Tax Security Awareness Week encourages individuals, businesses and tax professionals to secure their sensitive financial data. This can be a prime time for identity thieves seeking information they can use to file fraudulent tax returns.

Since 2015, the Internal Revenue Service has partnered with states and the tax industry to fight a common enemy – identity thieves. While much progress has been made, more work remains. National Tax Security Awareness Week, which started in 2016, is an opportunity for the Security Summit partners to work together and with other stakeholders to spread our security messages.

These messages can be used as part of the awareness campaign or any time during the 2020 filing season.

This toolkit provides key messages plus pre-written articles and/or emails that IRS partners and Security Summit participants can share with key at-risk groups threatened by identity theft: taxpayers, businesses and tax professionals. Partners can customize their own communications with these key messages or use the drop-in articles in newsletters or as email content.

Important note: *This information is not copyrighted, so your group can use this material and adjust it as needed. You can feel free to cite IRS or the Security Summit as a source for the material as needed.*

Schedule of Events

The IRS, through the Security Summit, will issue a series of news releases, tax tips and social media posts during this critical time, sharing key messages on real threats and basic steps that everyone can take. There will also be partnership news conferences to help spread the word via the media.

Tentative schedule:

- November 18 –National Tax Security Awareness Week Announcement
- December 2 – Cyber Monday tips on basic security steps
- December 3 – Identifying and avoiding phishing emails
- December 4 – How to create strong passwords
- December 5 – Businesses also can be identity theft victims
- December 6 – Tax professionals must have data security plans.

Goal: The idea behind the week is to leverage communications from multiple sources and on multiple platforms – with support of groups inside and outside the nation's tax community -- to increase the likelihood that taxpayers, tax pros and businesses receive the information. However, if this time frame does not fit your group's outreach plans, that's okay. These security messages are timely at any time of the year, including the 2020 filing season and after April 15.

What You and Your Group Can Do to Help

We're asking all our partners inside and outside the tax community to join with the Security Summit team to spread the word. Combating identity theft, especially in the cyber world, requires all of us working together to spread the word. For this ongoing effort, we will create communication products that partners can use as-is or adapt for their individual purposes – either during National Tax Security Awareness Week or other times of the year.

Sample Activities for National Tax Security Awareness Week Partners

- Hold a news conference.
- Adapt our generic news release and you can issue to the media/public
- Send an email to your employees, clients or customers
- Reproduce a ready-to-use article for online or print newsletters
- Share social media posts to Facebook, Twitter and/or Instagram.
- Issue a news release urging safe cyber practices.

Need Help with a Press Event or News Release?

Contact the IRS Media Relations Office for press conference and toolkit assistance at 202-317-4000.

Communication Resources

News Conference Script/Talking Points
(Adapt as needed for your group)

Often, representatives from several groups come together to use a news conference for local media. Below is a sample news conference script to help you provide basic information to help taxpayers, business and tax pros protect themselves against identity theft.

Key things to keep in mind:

- *The sample below is set up for five speakers. You can do an event with as little as one speaker or as many as you would like – simply adjust these as needed.*
- *Feel free to adjust this messaging to your local geographic area or your specific audience group. For example, Speaker 5 may be more appropriate if your event includes tax professionals.*

Speaker 1

We're here today to mark the 4th annual National Tax Security Awareness Week. This time of year is not only the holiday shopping season but also hunting season for identity thieves.

Thieves target your personal information so they can file fraudulent tax returns in your name. The IRS, state tax agencies and nation's tax industry – along with many other groups like those here today -- have been working together in partnership and have made great strides against tax-related identity theft. But more needs to be done.

Everyone has a role to play, and here are a few things you can do:

- To protect yourself online, take these basic steps:
    - Use security software for computers and mobile phones; keep it updated
    - Protect your personal information; don't hand it out to just anyone
    - Use strong and unique passwords for your accounts
    - Use two-factor authentication whenever possible
    - Shop only secure websites; Look for the "https" in web addresses; avoid shopping on unsecured and public wi-fi.
    - Back up your files on computers and mobile phones

Speaker 2 (Potential IRS or State tax partner when available)

The most common way identity thieves steal your information is through phishing emails. More than 90 percent of all data thefts start with a phishing email. Here's what you need to know:

- Remember a simple rule: Don't take the bait! Recognize and avoid phishing emails. These email scams often:
    - Pose as companies you know and trust, and
    - Tell an urgent story to trick you into opening link or attachment
- And, watch out for scam phone calls, too. No, that's not the IRS calling you out of the blue. Remember:
        - The IRS does not call demanding payment and making threats of jail or lawsuits
        - The IRS does not demand payment via gift or debit cards. The IRS and (local state) do not accept tax payments by iTunes cards.
        - The IRS does not send unsolicited emails about refunds or payments, requesting either login credentials, Social Security numbers or other sensitive information.

Speaker 3

One of the keys for protecting your online accounts – whether it involves taxes or anything else -- is to use strong passwords. Confused about how to create strong passwords?

- Here are some simple guidelines:
    - Use long phrases that you can remember, combined with characters and numbers, example: SomethingYouCanRemember@30.
    - Use a different password for each account; don't use your email address if that's an option and use a password manager.
    - Use two-factor authentication whenever it's offered, for example on email accounts, financial accounts and social media accounts.

Speaker 4

We often focus on individual taxpayers as victims of tax-related identity theft. But businesses also can be victims – and identity thieves love that they can reach more people's data through this route. Identity thieves steal businesses' Employer Identification Numbers, also called EINS, and use them to file false tax returns.

Businesses and tax professionals should contact the IRS if they experience any of these issues:

- An e-filed return is rejected because of a duplicate is already on file with the IRS.
- Routine extension-to-file requests are rejected.
- An unexpected receipt of a tax transcript or an IRS notice.
- Failure to receive expected and routine correspondence from the IRS, which can be an indicator an identity thief has changed the address.

Speaker 5

Finally, we call on all tax professionals to also act. Identity thieves increasingly target tax pros because of all the sensitive client data they hold. We urge tax professionals to review the Taxes-Security-Together Checklist issued by the IRS earlier this year. You can find it at IRS.gov/identitytheft.

Here are the five check list items for tax pros to keep in mind:

- Deploy basic security measures
- Create a written data security plan as required by law
- Educate yourself on phishing scams
- Recognize the signs of client data theft
- Create a data theft recovery plan

Speaker 1: Wrap Up

Finally, as the holidays approach, many of us will be with family and friends. And in a season of giving, keep in mind to look out for your friends and family members who could be at risk of identity theft. We all know someone who can be tech challenged – they can be any age or from any walk of life.

Encourage them to make sure they're being safe when they're on the web – make sure they have anti-virus software and a firewall. Make sure they're wi-fi is protected. Simple steps like these can not only protect their financial data, it could also help protect them when they file their tax return – and help ensure their tax refund gets to them as quickly as possible.

I just want to conclude our news conference with this message. In this era of data breaches, we all need to do everything we can to protect our sensitive financial information. This is critical to help protect your sensitive information that can be used to file a tax return in your name. Our message is to treat your data like your dollars; don't leave them lying around. Don't let your holidays – or your tax refund – be ruined by an identity theft Grinch during the holidays. Thank you.

Generic News Release for Completion by Partners

Partners and stakeholders can issue a news release as part of their news conference or as a stand-alone product. Media generally accept news releases via email. Make sure to obtain proper media contact information and to include your contact information should media request additional information. Simply insert your city and name of organization where noted by yellow highlights and then remove yellow highlights.

For release – Dec. 2 or later

Headline: (Name of Group) joins National Tax Security Awareness Week; Urges (city/state) residents to protect sensitive data as 2020 tax season approaches

(Name of City) (Name of your organization) today joined a nationwide campaign to mark the 4th annual National Tax Security Awareness Week, calling on people to step up their security safeguards against identity theft as the 2020 tax season approaches.

The holiday shopping season is the prime time for identity thieves who are trying to steal financial and personal data, either to drain credit/bank accounts or file fraudulent tax returns in the victims' names early in 2020.

(Name of your organization) is partnering with the Internal Revenue Service, state tax agencies, the nation's tax industry and other partners to elevate awareness around basic security steps. Remember, treat your data like your dollars; don't leave them lying around.

(Sample quote or use your own) "People in (name of city/state) should be extra careful this holiday season to protect their sensitive personal information. This information can be used by identity thieves to file false tax returns and many other things," said xxx. "Don't let this be a season of giving to identity thieves. Turn it into a season of protection for you, your family and your friends."

During this holiday season, there are basic steps people can easily overlook that they can take to protect themselves. These include:

- Shop at websites where the web address begins "https" – the "s" is for secure communications.
- Don't shop on unsecured public wi-fi in malls or hotels, where thieves can tap in.
- Secure you home wi-fi with a password.
- Use security software for computers and mobile phones; keep it updated.
- Protect your personal information; don't hand it out to just anyone.
- Use strong and unique passwords for your accounts.
- Use two-factor authentication whenever possible.

- Back up your files on computers and mobile phones.

Watch out for scam emails during holidays, tax season

The most common way thieves steal identities or account passwords is simply by asking for it through phishing emails. Remember, don't take the bait! Recognize and avoid phishing emails. These tricky scams often:

- Pose as companies you know and trust, including places like the IRS.
- These emails tell an urgent story to trick you into opening a link or an attachment, which can lead to adding a virus or spyware onto your computer.

And, no, that's not the IRS calling demanding a tax payment on a gift card. Remember:

- The IRS does not call demanding payment and making threats of jail or lawsuits
- The IRS does not demand payment via gift or debit cards. The IRS does not accept tax payments on iTunes cards. At tax time, checks should be addressed to "U.S. Treasury."
- The IRS does not send unsolicited emails about refunds or payments, requesting your login credentials, Social Security numbers or other sensitive information.

Just a few simple security steps can make all this different. Protect your data; protect your money and your financial information.

Contact: Name and Phone Number of Press Contact

###

Ready-to-Use Articles/Emails

Some partners/stakeholders may have newsletters (either print or electronic) or email lists of clients and employees. These communication products can double as either articles for newsletter or as email content to clients and/or employees. These cut-and-paste products are tailored for the National Tax Security Awareness Week, but these are good messages to share anytime during the 2020 filing season.

DECEMBER 2 – MONDAY – Message for Taxpayers

Article/Email #1 – 179 words

Cyber Monday Tips for Secure Shopping

As Cyber Monday kicks off the holiday shopping season, the Internal Revenue Service and its partners urged the public to shop safely by securing their computers and mobile phones.

The IRS, state tax agencies and the tax industry mark the fourth annual National Tax Security Awareness Week with tips on basic safeguards everyone should take, but especially for those shopping online via computer or mobile phone during the holiday season.

These basic protective steps include:

- Shop at sites where the web address begins “https” – the “s” is for secure communications.
- Don’t shop on unsecured public wi-fi, thieves can eavesdrop; secure you home wi-fi with a password.
- Use security software for computers and mobile phones; keep it updated.
- Protect your personal information; don’t hand it out to just anyone.
- Use strong and unique passwords for your accounts.
- Use two-factor authentication whenever possible.
- Back up your files on computers and mobile phones.

Note the recommendations include security measures for mobile phones. Thieves have become more adept at compromising mobile phones. You should protect your mobile phones as you do your computers.

December 3 – TUESDAY – Message for Taxpayers

Article/Email #2 – 249 words

Don't take the bait: Recognize and Avoid Phishing Scams

This holiday season don't let the cyber grinches steal your money or your identity. The Internal Revenue Service, state tax agencies and the nation's tax industry are working together to protect taxpayers from stolen identity refund fraud. All this week, the Security Summit partners will be sharing tips as part of the National Tax Security Awareness Week. But the partners need your help.

Here's what you need to know to protect yourself from phishing scams:

First, the most common way thieves steal your identity is simply by asking for it. Their favorite tactic is a phishing email. Phishing emails bait you into opening them. They pose as a trusted company - maybe your bank, a favorite retailer or your tax provider.

Second, learn to recognize and avoid them. The scams tell an urgent story – i.e. there's a problem with your account – and instructs the receiver to open an embedded link or download an attachment.

Third, don't take the bait. The link may send you to a familiar website to login, but your username and password goes to the thieves. Or, the scam suggests you open an attachment, which secretly downloads malicious software. Either are bad news. Just hit delete.

And no, that's not the IRS calling with demands of payment and threats of jail or a lawsuit. The IRS does not make angry, threatening phone calls. Nor does the IRS request payment via gift cards or debit cards, like iTunes cards. Always make your payment to the U.S. Treasury.

December 4 – Wednesday – Message for Taxpayers

Article/Email #3

How to Create Strong Passwords – 310 words

A commonly overlooked step to protecting your personal tax and financial data is using strong passwords to protect online accounts and digital devices from data theft.

The Internal Revenue Service, state tax agencies and tax industry remind taxpayers that using strong passwords and keeping them secure are critical steps to preventing thieves from stealing identities or money. This is just one of a series of tips offered this week as part of the National Tax Security Awareness Week.

In recent years, cybersecurity experts' recommendations on what constitutes a strong password has changed. They now suggest that people use word phrases that are easy to remember rather than random letters, characters and numbers that cannot be easily recalled. A new example: SomethingYouCanRemember@30.

Protecting access to digital devices is so critical that some are now using fingerprint or facial recognition technology. But if you are still using password protections, consider these tips to protect devices or online accounts.

- Use a minimum of eight characters; longer is better.
- Use a combination of letters, numbers and symbols, i.e., XYZ, 567, !@#.
- Avoid personal information or common passwords; opt for phrases.
- Change default/temporary passwords that come with accounts or devices.
- Do not reuse passwords, e.g., changing Bgood!17 to Bgood!18 is not good enough; use unique usernames and passwords for accounts and devices.
- Do not use email addresses as usernames, if that is an option.
- Store any password list in a secure location, such as a safe or locked file cabinet.
- Do not disclose passwords to anyone for any reason.
- Use a password manager program to track passwords if you have numerous accounts.

Whenever it is an option for a password-protected account, users also should opt for a multi-factor authentication process. Many email providers, financial institutions and social media sties now offer customers two-factor authentication protections, which adds an extra layer of protection for your accounts.

December 5 – THURSDAY – Message for Businesses

Article/Email #4 – 240 words

Cyberthieves Target Businesses of All Sizes

Employers large and small must be alert to the growing threat of business identity theft and take additional steps step up cybersecurity protections.

Awareness about business identity theft is one in a series of tips offered by the Internal Revenue Service, state tax agencies and tax industry, which work together as the Security Summit to protect taxpayers. The Security Summit is marking its fourth National Tax Security Awareness Week by reminding employers that they too can be victims of identity theft.

As with fraudulent individual returns, there are certain warning signs that may indicate identity theft. Business, partnerships and estate and trust filers should be alert to potential identity theft and contact the IRS if they experience any of these issues:

- Extension to file requests are rejected because a return with the Employer Identification Number (EIN) or Social Security Number (SSN) is already on file;
- An e-filed return is rejected because of a duplicate EIN/SSN is already on file with the IRS;
- An unexpected receipt of a tax transcript or an IRS notice or letter that doesn't correspond to anything submitted by the filer;
- Failure to receive expected and routine correspondence from the IRS because the identity thief has changed the address.

The IRS also asks those tax professionals preparing business-related returns to step up the "know your customer" procedures. Tax preparation software for business-related returns asks a series of questions. Answering those questions also will help identify suspicious returns.

December 6 – FRIDAY – Message for Tax Pros

Article/Email #5 – 293 words

Tax Practitioners Must Draft Written Data Protection Plans

The IRS, state tax agencies and the nation's tax industry today reminded tax professionals that federal law requires them to create and use a written information security plan to protect their clients' data.

The reminder came as the IRS and its Security Summit partners completed the fourth annual National Tax Security Awareness Week. The special week's purpose is to encourage individuals, businesses and tax professionals to take steps to protect sensitive financial and tax data that can be used by identity thieves.

To get started on an information security plan, tax professionals can review IRS Publication 4557, Safeguarding Taxpayer Data (PDF). It details critical security measures that all tax professionals should take. The publication also includes information on how to comply with the Federal Trade Commission (FTC) Safeguard Rule.

Regardless of size, each tax firm, as part of its plan, must:

- designate one or more employees to coordinate its information security program;
- identify and assess the risks to customer information in each relevant area of the company's operation and evaluate the effectiveness of the current safeguards for controlling these risks;
- design and implement a safeguards program and regularly monitor and test it;

- select service providers that can maintain appropriate safeguards, make sure the contract requires them to maintain safeguards and oversee their handling of customer information; and
- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

Earlier this year, the Security Summit partners offered tax professionals a Taxes-Security-Together Checklist to consider. The Summit partners renewed their call for tax professionals to stop and review the safeguards prior to the start of the 2020 filing season and to take appropriate steps to protect their clients – and themselves.

IRS Videos

Partners or media are free to download and share any IRS YouTube videos.

- IRS Commissioner Urges Taxpayers to Protect Their Data
- Easy Steps to Protect Your Computer and Phone
- Avoid Phishing Emails

Publications/Web links

- IRS Publication 4524, Security Awareness for Taxpayers
- IRS Publication 4557, Safeguarding Taxpayer Data
- IRS Publication 5293, Data Security Resource Guide for Tax Professionals
- IRS Identity Protection, Detection and Victim Assistance – IRS.gov/identitytheft
- Small Business Information Security – the Fundamentals
- Start with Security: A Guide for Business – Federal Trade Commission

Sharable Social Media

To supplement the awareness campaign, there are social media posts available for sharing throughout the week or the 2020 filing season, including posts in multiple languages. Please follow the hashtag **#TaxSecurity** *on the IRS social media accounts.*

- Twitter: @IRSnews, @IRStaxpros, @IRSenEspanol, @IRStaxsecurity, @IRSsmallbiz
- Facebook: IRS and IRS en Español
- LinkedIn: Internal Revenue Service
- Instagram: @IRSnews

News Releases

During the National Tax Security Awareness Week, the IRS will issue daily news releases in both English and Spanish. Below is a summary highlight of those news releases. The messages parallel other products in this toolkit. The IRS will share these news release in separate attachments.

December 2
National Tax Security Awareness Week begins; IRS and Security Summit partner offer Cyber Monday shopping tips to protect computers, mobile phones

WASHINGTON – The Internal Revenue Service and the Security Summit partners opened this year's National Tax Security Awareness Week with a warning for holiday shoppers on Cyber Monday to secure their computers and mobile phones to reduce the threat of identity theft.

During the holiday season, criminals take advantage of large numbers of people shopping online to steal identities and money – as well as sensitive tax and financial data that can be used to file fraudulent tax returns when the filing season opens in early 2020.

December 3
National Tax Security Awareness Week, Day 2: Don't take the bait: Recognize, avoid phishing scams from identity thieves

WASHINGTON – As the holiday season approaches, the IRS and Security Summit partners warned taxpayers to watch out for phishing scams in the deluge of holiday email messages coming from retailers and others.

More than 90 percent of all data thefts begin with an email phishing scam. The IRS, state tax agencies and the nation's tax industry – working together as the Security Summit -- warned people to watch out for phishing scams during the busy holiday shopping period and in advance of the 2020 tax season.

December 4
National Tax Security Awareness Week, Day 3: Creating strong passwords can protect taxpayers from identity theft

WASHINGTON – With millions of people logging in to online websites and accounts this holiday season, the IRS and the Security Summit partners remind taxpayers that

common mistakes can increase their of risk having sensitive financial and tax data stolen by identity thieves.

The Internal Revenue Service, state tax agencies and the nation's tax industry remind taxpayers that using strong passwords and keeping them secure are critical steps to preventing thieves from stealing identities, money or using the information to file a fraudulent tax return.

December 5

National Tax Security Awareness Week, Day 4: IRS, Security Summit warns business owners about being a target for identity thieves

WASHINGTON – Amid threats from cybercriminals, the IRS, state tax agencies and the tax industry urged employers large and small to step up cybersecurity protections against business identity theft.

Identity thieves are displaying a sophisticated knowledge of the tax code and industry filing practices as they attempt to obtain valuable data to help file fraudulent returns. To address this and protect taxpayers and their business returns, the IRS has taken steps to identify and prevent business identity theft.

December 6

National Tax Security Awareness Week, Day 5: Tax professionals need data protection plans; must guard against identity theft

WASHINGTON – As National Tax Security Awareness week concludes, the IRS, state tax agencies and the tax industry today reminded tax professionals that federal law requires them to create and follow a written information security plan to protect their clients' data.

The reminder came as the IRS and its Security Summit partners today completed the fourth annual National Tax Security Awareness Week. The purpose of the week-long educational effort is to encourage individuals, businesses and tax professionals to take steps to protect sensitive data, including their identities and personal information.

###

Thank You from Chuck Rettig

The IRS, state tax agencies and the nation's tax industry appreciate your efforts to protect the nation's taxpayers – and their identities. Any action your organization can take to share this information will make a difference. We hope you find this toolkit helpful. If you have any suggestions on how we can improve this toolkit or our campaign to protect taxpayers, please email newsroom@irs.gov to share your thoughts.

Sincerely,

Chuck Rettig, Commissioner, Internal Revenue Service