IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

IRS warns of holiday scams, encourages protecting sensitive personal information as 9th annual National Tax Security Awareness Week starts

IR-2024-300, Dec. 2, 2024

WASHINGTON — On Cyber Monday, the Internal Revenue Service and its Security Summit partners warned taxpayers to approach their holiday shopping with extra caution because scammers are also shopping – for their next victim's personal information.

The consumer alert kicks off the ninth annual National Tax Security Awareness Week featuring tips for taxpayers and tax professionals to avoid scams and protect their sensitive data. The special week is part of the Security Summit initiative, a joint effort between the IRS, states, the tax industry and tax professionals that works to protect taxpayers and the tax system against identity theft.

"The holiday shopping season and the fast-approaching tax season create a tempting target for identity thieves and scam artists," said IRS Commissioner Danny Werfel. "Taxpayers should use extra caution this holiday season to protect their valuable personal and financial information, whether shopping online or clicking on links in email and other messages. A little extra caution can protect taxpayers' confidential information and reduce the risk of identity theft in the upcoming filing season."

Abundant scams and rip-offs being seen by the IRS and the Security Summit partners include ever-evolving and increasingly sophisticated phishing emails and related attacks on the unsuspecting. Taxpayers can be duped into unwittingly handing over their confidential tax and financial information. Would-be victims could also get tricked into disclosing their addresses, Social Security numbers, bank account numbers, credit card numbers or passwords, which can lead to tax-related identity theft and fraud.

A common example right now involves false messages made to look like they're coming from delivery services. In these scams, victims receive a text or email purporting to be from a company or business saying a delivery can't be made along with a link to click to reschedule. But in reality, the link represents a form of phishing that attempts to steal personal information or download malware. It's a very prevalent scam expected to intensify during the holidays.

Another common scam expected to intensify soon will involve emails pretending to be from the IRS or others in the tax industry. These frequently involve unexpected, good news, like a tax refund. But they can also involve variants telling people they have a tax bill or have tax documents available to download.

"People need to be extra careful during the holidays and during tax season," Werfel said. "Identity thieves and tax scammers are shrewd and take advantage of what is on people's minds, particularly during busy times of the year like the holidays. Remember, don't click on anything unknown, even if you just ordered gifts and you're expecting packages to come to your door soon. Double-check before you click."

The warning is another reminder from the IRS and other Security Summit partners, an ongoing alliance that includes state tax agencies, tax professionals, software and financial industry partners. Since 2015, the IRS and the Security Summit have used this special week to warn taxpayers and tax professionals to protect their sensitive information while shopping online or viewing emails and texts, especially during the holiday season and approaching tax season, when criminals are active.

The Summit partners continue to highlight security and awareness to help taxpayers avoid losing their personal, financial and tax information, which identity thieves use to file fraudulent tax returns.

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

Safety tips to remember during the holiday season and throughout the year

During the busiest time of the year for online shopping, the Security Summit reminds taxpayers of some important steps to protect themselves and their information from data thieves:

- Shop at online sites with web addresses that begin with the letters “https:” the “s” stands for secure communications. Also look for a padlock icon in the browser window.
- Don't shop on unsecured public Wi-Fi in places like a mall or restaurant.
- Ensure security software is updated on computers, tablets and mobile phones.
- Watch out and help protect the devices of family members who may not be technologically savvy, a wide range that goes from young children to older adults.
- Make sure anti-virus software for computers has a feature to stop malware, and that there is a firewall enabled to prevent intrusions.
- Use strong, unique passwords for online accounts.
- Use multi-factor authentication whenever possible.

Simple steps can protect taxpayers

In addition to those protective steps, taxpayers should be wary of a variety of email scams. Throughout the year, taxpayers should be aware of different types of email phishing scams that identity thieves and scam artists commonly use. These include:

- Phishing/Smishing – Phishing emails or SMS/texts (known as “smishing”) attempt to trick a recipient into clicking a suspicious link, filling out information or downloading a malware file. Often phishing attempts are sent to multiple email addresses at a business or agency, increasing odds that someone will fall for the trick.
- Spear phishing – This is a specific type of phishing scam that bypasses emailing large groups at an organization, instead identifying potential victims and delivering a more realistic email known as a “lure.” These types of scams can be trickier to identify since they don't occur in large numbers. They single out individuals, can be specialized and make the email seem more legitimate. Scammers can pose as a potential client for a tax professional, luring the practitioner into sharing sensitive information.
- Clone phishing – This is a newer type of phishing scam that clones a real email message and resends it to the original recipient pretending to be the original sender. The new message will have either an attachment that contains malware or link that tries to steal information from a recipient.
- Whaling – Whaling attacks are very similar to spear phishing, except these attacks are generally targeted to leaders or other executives with access to large amounts of information at an organization or business. Whaling attacks can target people in payroll offices, human resource personnel and financial offices as well as leadership.

In some cases, when a taxpayer believes their personal information is being used to file fraudulent tax returns, they should consider filing a Form 14039 online, or they can complete the paper Form 14039, Identity Theft Affidavit, which can then be printed and mailed or faxed to the IRS.

This is the first part of a week-long series of tips to raise awareness about identity theft. Go to National Tax Security Awareness Week 2024 for additional information.

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

Additional resources

For more information on preventing tax information theft, visit Security Summit.

Victims of identity theft can visit Identity Theft Central.

Find additional information on tax scams at Tax scams.

Attend the IRS and Federal Trade Commission webinar: Scams, tax related identity theft and Identity Protection PIN for National Tax Security Awareness Week on Tuesday, Dec. 3, at 11 a.m. ET. Register by visiting the webinar information page.

A tax security awareness social media toolkit is available on IRS.gov with sample text and graphics to help promote #TaxSecurity on social media channels. The toolkit is also available on National Tax Security Awareness Week 2024 under Helpful Resources.

Get other reliable tax info from the following trusted sources:

- Follow IRS on social media.
- Visit an IRS walk-in center.
- Talk to a trusted tax professional.

-30-