



# Rhode Island Department of Revenue

## Division of Taxation

ADV 2021-46  
SECURITY SUMMIT

ADVISORY FOR TAXPAYERS AND TAX PROFESSIONALS  
NOVEMBER 29, 2021

### Security Summit provides tips to foil identity thieves

*This holiday season, protect yourself and your family*

PROVIDENCE – The Rhode Island Division of Taxation, the Internal Revenue Service (IRS), and the tax industry – working together as the Security Summit – have launched the 6th annual National Tax Security Awareness Week to protect against identity theft with basic safeguards everyone should take.

The Rhode Island Division of Taxation, the Internal Revenue Service, and other partners in the Security Summit warn taxpayers and tax professionals to beware of a dangerous combination of events that can increase their exposure to tax scams or identity theft.



Criminals have numerous opportunities to steal sensitive personal or financial information due to the combination of the holiday shopping season, the upcoming tax season, and the pandemic.

Security Summit partners advise taxpayers to take extra care with their online activities. For example, many criminals steal personal data when shoppers use their phones to make purchases over unsecured Wi-Fi networks. People should take extra care while shopping online or

viewing emails and texts.

To help taxpayers and tax professionals, the Security Summit shared 10 basic steps everyone should remember during the holidays and as the 2022 tax season approaches.

#### 10 Key Steps to Protect Sensitive Information:

- Don't forget to use security software for computers, tablets, and mobile phones – and keep it updated. Protect electronic devices of family members, especially teens and young children.
- Make sure anti-virus software for computers has a feature to stop malware, and there is a firewall enabled that can prevent intrusions.
- Phishing scams – like imposter emails, calls, and texts -- are the No. 1 way thieves steal personal data. Don't open links or attachments on suspicious emails. This year, fraud scams related to COVID-19, Economic Impact Payments and other tax law changes are common.
- Use strong and unique passwords for online accounts. Use a phrase or series of words that can be easily remembered or use a password manager.
- Use multi-factor authentication whenever possible. Many email providers and social media sites offer this feature. It helps prevent thieves from easily hacking accounts.

- Shop at sites where the web address begins with "https" – the "s" is for secure communications over the computer network. Also, look for the “padlock” icon in the browser window.
- Don't shop on unsecured public Wi-Fi in places like a mall. Remember, thieves can eavesdrop.
- At home, secure home Wi-Fis with a password. With more homes connected to the web, secured systems become more important, from wireless printers and wireless door locks to wireless thermometers. These can be access points for identity thieves.
- Back up files on computers and mobile phones. A cloud service or an external hard drive can be used to copy information from computers or phones – providing an important place to recover financial or tax data.
- Working from home? Consider creating a virtual private network (VPN) to securely connect to your workplace.



The Security Summit also provided these warning signs to increase taxpayer awareness of scams and data-theft operations:

- Identity thieves continue to try to look like government agencies and others in the tax community by emailing or texting about tax refunds, stimulus payments or other items. The IRS will not call or send unexpected texts or emails about things like refunds. More information about these common scams is available at [IRS Tax Tip: Common tax scams and tips to help taxpayers avoid them](#).
- Remember - these security measures include mobile phones, an area that people sometimes can overlook. Thieves have become more adept at compromising mobile phones. Phone users also are more prone to open a scam email from their phone than from their computer. Taxpayers can check out security recommendations for their specific mobile phone by reviewing the Federal Communications Commission's [Smartphone Security Checker](#). Since phones are used for shopping and even for doing taxes, remember to make sure phones and tablets are just as secure as computers.
- During the pandemic, there continue to be numerous scams related to COVID-19. These can be attempts to gain sensitive personal or financial information. The Federal Trade Commission also has issued [alerts](#); consumers can keep atop the latest scam information and report COVID-related scams.

#### **About the Security Summit**

The Security Summit consists of the IRS, state tax agencies, and the tax community -- including tax preparation firms, software developers, processors of payroll and tax financial products, tax professional organizations, and financial institutions. Partners in the Security Summit help protect taxpayers from identity theft and refund fraud. See <https://www.irs.gov/newsroom/security-summit> for more details.

---

*The Rhode Island Division of Taxation is open to the public from 8:30 a.m. to 3:30 p.m. business days. For more information, contact the Division of Taxation at (401) 574-8829 or see <http://www.tax.ri.gov/contact/>.*

---