ADV 2020-52
SECURITY SUMMIT

ADVISORY FOR TAXPAYERS AND TAX PROFESSIONALS
NOVEMBER 30, 2020

Beware of scams and identity theft schemes, Security Summit says

Criminals try to take advantage amid holiday shopping and upcoming filing season

PROVIDENCE — The Rhode Island Division of Taxation, the Internal Revenue Service, and other partners in the Security Summit today warned taxpayers and tax professionals to beware of scams and identity theft schemes by criminals who seek to take advantage of holiday shopping, the approaching tax season, and coronavirus (COVID-19) concerns.

The IRS, state tax agencies, and the tax industry today opened National Tax Security Awareness Week to coincide with Cyber Monday, the traditional start of the online holiday shopping season. But the holiday shopping season, combined with the upcoming tax season, and an increased trend toward working remotely, make online security an absolute necessity.

"This is generally the hunting season for online thieves, but this year there's a dangerous combination of factors at play that should make people more alert," said IRS Commissioner Chuck Rettig.

"The combination of online holiday shopping, the approaching filing season, and more of us working remotely, puts people more at risk. People can help avoid becoming victims of scams or identity thefts by taking a few simple steps to help protect sensitive tax and financial information," said Rhode Island Tax Administrator Neena Savage.

Basic steps

Following are a few basic steps everyone should remember during the holidays and as the 2021 tax season approaches:

- Don't forget to use security software for computers and mobile phones – and keep it updated.
- Make sure purchased anti-virus software has a feature to stop malware, and make sure there is a firewall that can prevent intrusions.
- Phishing scams – like imposter emails, calls, and texts -- are the top way thieves steal personal data. Don't open links or attachments on suspicious emails. This year, fraud scams related to COVID-19 and the "economic impact payments" (sometimes called "stimulus payments", "COVID-19 payments", or "recovery rebates") 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 prevents 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, such as a mall. Remember, thieves can eavesdrop.
- At home, secure your home Wi-Fi with a password. With more homes connected to the web, secured systems become more important, from wireless printers to wireless door locks and 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 partners also note that security measures should extend to 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" through the following link: https://www.fcc.gov/smartphone-security. Because phones are used for shopping and even for doing taxes, remember to make sure phones and tablets are just as secure as computers.

Neither the Rhode Island Division of Taxation nor the IRS will call, text, or email you about your federal Economic Impact Payment or your federal or state tax refund. Neither the Rhode Island Division of Taxation IRS will call with threats of jail or lawsuits over unpaid taxes. Those are scams.

The Federal Bureau of Investigation issued warnings earlier about fraud and scams related to the pandemic. It specifically warned of COVID-19 schemes related to taxes, anti-body testing, healthcare fraud, cryptocurrency fraud, and others. COVID-related fraud complaints can be filed at the National Center for Disaster Fraud at: https://www.justice.gov/disaster-fraud.

The Federal Trade Commission also has issued alerts about fraudulent emails claiming to be from the Centers for Disease Control or the World Health Organization. Consumers can keep atop the latest scam information and report COVID-related scams at www.FTC.gov/coronavirus.

The Security Summit consists of the IRS, the Rhode Island Division of Taxation, other states' tax agencies, and the tax community -- including tax preparation firms, software developers, tax professional organizations, and financial institutions. Partners in the Security Summit work together to combat identity theft and fight other scams to protect the nation's taxpayers. To learn more about the Security Summit: https://www.irs.gov/newsroom/security-summit.