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 ...

Dec. 01, 2020

The Internal Revenue Service and the Security Summit partners have issued warnings to all taxpayers and tax professionals to beware of scams and identity theft schemes by criminals taking advantage of the combination of holiday shopping, the approaching tax season and coronavirus concerns.

The IRS, state tax agencies and the tax industry opened the 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

impending tax season and an increased trend toward working remotely make online

The IRS, state tax agencies and the nation's tax industry – working together as the Security Summit – mark the start of the 5th annual National Tax Security Awareness Week with tips on basic safeguards everyone should take.

The special week includes special informational graphics and social media efforts on platforms including Twitter and Instagram.

Here 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 there is a firewall 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 and the Economic Impact Payment 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 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, wireless

door locks to wireless thermometers. These can be access points for identity

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.

The IRS will not call, text or email about your Economic Impact Payment or your tax refund. Nor will the IRS 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.

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 IRS, state tax agencies, the private sector tax industry, including tax professionals, work in partnership as the Security Summit to help protect taxpayers from identity theft and refund fraud. This is the first in a week-long series of tips to raise awareness about identity theft. See IRS.gov/securitysummit for more details.

Digital Currency