NATIONAL CYBERSECURITY ALLIANCE

Stay Safe Online During Tax Time

TAX SCAM DIRTY DOZEN

The IRS includes a "Dirty Dozen" recap of scams on its website, including the top two ploys listed to the right, and others others like tax preparer fraud, fake charities and inflated refund claims. Check it out here: https://www.irs.gov/newsroom/dirty-dozen

In 2018, the Internal Revenue Service (IRS) noted an astonishing 60 percent increase in bogus email schemes that seek to steal money or tax data.

Beware of:

- ***Unsolicited emails, text messages, social media posts or fake websites that prompt you to click on a link or to share valuable personal and financial information.*** Armed with this information, online thieves can swindle funds and/or commit identity theft. Unfamiliar links or attachments can also contain malware – viruses, spyware and other unwanted software that is installed on your computer or mobile device without your consent.

- ***Unscrupulous callers claiming to be IRS employees*** using fake names and phony ID numbers. They may ring you and insist that you owe money and that it must be paid as soon as possible through a gift card or wire service. If the call is not picked up, the scammers often leave an emergency callback request message. In reality, the IRS rarely calls taxpayers and initiates almost all contact via the U.S. Postal Service.

TAX-TIME SECURITY TAKE-ACTION TIPS

When in doubt, throw it out: Criminals can get access to your personal information by tricking you into downloading attachments or clicking on links in email. If an email seems suspicious, even if you know the source, it's best to delete.

Lock Down Your Login. Create long and unique passphrases for all accounts and use multi-factor authentication (MFA) wherever possible. MFA will fortify your online accounts by enabling the strongest authentication tools available, such as biometrics or a unique one-time code sent to your phone or mobile device. Most major email and online tax preparing services have this tool available.

NATIONAL CYBERSECURITY ALLIANCE

Stay Safe Online During Tax Time

TAX-TIME SECURITY TAKE-ACTION TIPS

Get savvy about Wi-Fi hotspots: Public wireless networks are not secure. If you are filing your taxes online make sure you are doing it on a secure and personal network.

Think before you act: Be leery of communications that implore you to act immediately – especially if you are told you owe money to the IRS and it must be paid promptly.

Do your research. Vet your tax preparer before handing over sensitive information. Ask what steps they take to protect your information. Businesses of all sizes are susceptible to cyberthieves, so it is critical you choose a preparer who takes your security seriously.

Update your software. Before filing your taxes at home or work, be sure that all internet-connected devices –including PCs, smartphones and tablets – are running the most current versions of software. Updates include important changes that improve the performance and security of your devices.

RESOURCES TO HELP YOU STAY SAFE THIS TAX SEASON

- ☑ STOP. THINK. CONNECT.™ Tips and Advice: https://stopthinkconnect.org/tips-advice
- ☑ Identity Theft Resource Center: https://www.idtheftcenter.org/tax-identity-theft/
- ☑ Federal Trade Commission: https://www.consumer.ftc.gov/features/tax-identity-theft-awareness
- ☑ IRS's Tax Scams and Consumer Alerts: https://www.irs.gov/newsroom/tax-scams-consumer-alerts
- ☑ Tax Security 2.0 – A "Taxes-Security-Together" Checklist: https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist