STAY SAFE ONLINE DURING TAX TIME

The National Cyber Security Alliance (NCSA) reminds Americans that with tax day just two months away, it is cybercriminals’ favorite time of the year. ‘Tis the season for online scams with phishing emails and fraudulent phone calls at the top of the list.

In 2018, the Internal Revenue Service’s (IRS) noted an astonishing 60 percent increase in bogus email schemes that seek to steal money or tax data. Cybercriminals will try to get you to do something so they can rob your personal information. 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. Malware is intentionally designed to wreak havoc on and infect your computer files in a variety of ways.

In addition, unscrupulous callers claiming to be IRS employees – using fake names and phony ID numbers – 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.

The IRS includes a “Dirty Dozen” recap of scams on its website, including the top two ploys listed above and others like tax preparer fraud, fake charities and inflated refund claims.

PROTECT AGAINST FRAUDSTER TRICKS WITH NCSA’S “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: Thwart thieves by enabling the strongest authentication tools available, often called multi-factor or two-factor authentication. Most major email and online tax preparing services have this tool available.
- 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.
- Ask if your tax preparation service has checked for malware issues and if your tax preparer’s business is cybersecure. Businesses of all sizes are susceptible to cyberthieves so it is critical they have a strong cybersecurity posture by following these NCSA-recommended steps.

"With tax filing in full swing, cyber crooks are doing everything they can to take full advantage of the opportunity,” said Kelvin Coleman, NCSA’s executive director. “Tax time is a haven for hackers, who are masters of manipulation. With the tremendous inventory of personal and financial shared online, it’s essential to remember that Personal Information Is Like Money. Value It. Protect It. Following good cybersecurity practices during tax season and throughout the year allows everyone to reap the benefits of connectivity with increased confidence."

RESOURCES TO HELP YOU STAY SAFE THIS TAX SEASON

- STOP. THINK. CONNECT."™ Tips and Advice
- Identity Theft Resource Center
- Federal Trade Commission
- The Internal Revenue Service’s Tax Scams and Consumer Alerts

STAYSAFEONLINE.ORG @STAYSAFEONLINE F STAYSAFEONLINE