STOP | THINK | CONNECT™

STAY SAFE FROM CYBERCRIME DURING TAX TIME

Tax season is prime time for online scams!

With the April 15 filing deadline just two months away, cybercriminals are looking to lift your personal information to cash in on a refund request and/or steal your identity.

The problem is rampant and cyber thieves are crafty: they can break into your account or device and literally steal your online life – as well as your tax refund.

Don't Become a Victim: Watch Out for Tax Season Tricks

Online con artists will tempt you to take action in a variety of ways. Beware of the following:

- **Phishing scams:** Cybercriminals will try to get you to do something, like click on a link or respond to an email, so they can steal your personal information. Watch out for unsolicited emails, texts, social media posts or fake websites that may lure you in and prompt you to share valuable personal and financial information. Armed with this information, online thieves can pilfer funds and/or commit identity theft. And opening malicious links or attachments can cause malware – viruses, spyware and other unwanted software that gets installed on your computer or mobile device without your consent – to infect your computer files.

- **Imposters claiming to be Internal Revenue Service (IRS) agents:** The IRS will never email or call you demanding immediate payment without having first mailed a bill – nor will they ask for a credit or debit card number via email or phone.

- **Tax preparer fraud:** The overwhelming majority of tax preparers provide honest services, but some unscrupulous individuals may target unsuspecting taxpayers and the result can be refund fraud and/or identity theft. The IRS reminds anyone filing a tax return, that the preparer must sign it with their preparer tax identification number.

Stay Cyber Safe – Follow These Tax Season Tips

The National Cyber Security Alliance (NCSA) has some easy-to-use STOP. THINK. CONNECT. tips that will help protect you against fraudster tricks.

- **Keep all machines clean:** Having updated software on all devices that connect to the Internet is critical. This includes security software, web browsers and operating systems for PCs and your mobile devices. Having current software is a strong defense against viruses and malware that can steal login credentials or potentially use your computer to generate spam.

- **Get two steps ahead:** Turn on two-step authentication – also known as two-step verification or multi-factor authentication – on accounts. Many popular email services and financial institutions offer this key security step for free, but you must opt in to turn it on.

- **Make better passwords:** If your passwords are too short or easy to guess, it's like giving a cyber thief your banking PIN. Longer passwords and those that combine capital and lowercase letters with numbers and symbols provide better protection.

Created by the National Cyber Security Alliance

- **Get savvy about Wi-Fi hotspots:** Public wireless networks are not secure. Cybercriminals can potentially intercept Internet connections while you are filing highly personal information on public WiFi.
- **When in doubt, throw it out:** Links in email are often the way bad guys get access to your personal information. If it looks weird, even if you know the source, it's best to delete.
- **Think before your 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.
- **File your tax forms on secure https sites only.**
- **Ask if your tax preparation service has checked for malware issues.**

Reminder from NCSA

"Cybercriminals can't wait for tax season. The flood of personal and financial data that's available online during this time of the year is a tremendous target. Everyone is filing their taxes, deadlines are looming and the bad guys are doing everything they can to take full advantage of the opportunity," said Michael Kaiser, NCSA's former executive director. "Hackers are masters of social engineering. So during timeframes when there is increased potential to have your most personal data exposed, it's critically important to take steps to use the Internet safely and more securely. Remember that *Personal Information Is Like Money. Value It. Protect It.* Practicing good cybersecurity – when preparing your tax returns and all year-round – empowers Internet users to reap the benefits of connectivity with greater confidence."

Resources to Help You Stay Safe this Tax Season

- Better Business Bureau shares 6 Tips for Trusting Your Tax Preparer, visit bbb.org/tax-us to learn more.
- Visit consumer.ftc.gov/articles/0008-tax-related-identity-theft for consumer-focused information about tax-related identity theft.
- IdentityTheft.gov can help you report and recover from identity theft.
- If you are a victim of identity theft, the Identity Theft Resource Center (idtheftcenter.org) can offer advice tailored to your specific issue, a step-by-step plan and the necessary documents and letters you will need to implement your plan.
- The Internal Revenue Service offers fool-proof tips for filing taxes online; visit irs.gov/Filing to learn more.
- Tax time is open season for ID thieves and IRS impersonators. Learn more about common scams at fraud.org/scams

FOLLOW US ONLINE AND ON SOCIAL MEDIA

STOP | THINK | CONNECT™

STOPTHINKCONNECT.ORG

@STOPTHNKCONNECT

/STOPTHINKCONNECT

STOPTHINKCONNECT

Created by the National Cyber Security Alliance