NATIONAL CYBERSECURITY ALLIANCE

ITRC IDENTITY THEFT RESOURCE CENTER

SIMPLE CYBERSECURITY TIPS FOR STAYING SAFE ONLINE DURING TAX TIME

Tuesday, April 18 might feel far-off, but the tax filing deadline will be here before you know it. That also means it's primetime for cyber thieves and their devious online scams. Tax identity theft – which occurs when someone uses your Social Security number to file a tax return and then steals your refund – is on the rise. According to the Federal Trade Commission (FTC), there was a nearly 50 percent increase in identity theft complaints in 2015, and by far the biggest contributor to the surge was the spike in tax refund fraud.[1] At this time last year, the Internal Revenue Service (IRS) reported a 400 percent increase in email phishing and malware incidents aimed at both taxpayers and tax professionals.[2] Cyber crooks are crafty: they can break into your account or device and literally steal your digital life – and your money. The National Cyber Security Alliance (NCSA) and Identity Theft Resource Center (ITRC) have teamed up to share cautionary tips for spotting cyber tricks, proactive online safety steps and invaluable advice about how to get help if you fall victim to tax identity theft.

DON'T BECOME A VICTIM: WATCH OUT FOR TAX SEASON TRICKS

Online outlaws will attempt to lure you in a variety of ways. Watch out for the following:

- **Fraudulent tax returns:** The FTC recommends trying to file your tax return as soon as possible. The IRS only accepts one tax return per Social Security number. If the file is yours and it's in early, it makes it impossible for a cyber thief to submit another return with your personal information. It's also important to always use smart practices with your personal information. Remember to only share your Social Security number when it's absolutely necessary. Check your credit report regularly for shady activity and never throw papers with critical information – like your Social Security number or bank account information – in the trash. It's best to shred all paper containing personal data.[3]

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

- **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 their preparer must sign it with their IRS Preparer Identification Number.

STAY CYBER SAFE – PRACTICE NCSA'S TAX SEASON TIPS

NCSA has some easy-to-use STOP. THINK. CONNECT.™ tips to 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 logon credentials or potentially use your computer to generate spam.
- **Lock down your login:** Fortify your online accounts by enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Your usernames and passwords are not enough to protect key accounts like email, banking and social media.
- **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.
- **Get savvy about WiFi 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.**

IF YOU THINK YOU'RE A VICTIM...

Follow these ITRC tips to get help as a victim of tax identity theft:

- **If you suspect identity theft:** If you think you have tax issues related to identity theft, contact the IRS immediately, even if you don't have any evidence that it has affected your tax return. You can call the IRS Identity Protection Specialized Unit (IPSU) at 1-800-908-4490.
- **File an ID Theft Affidavit:** You can document the identity theft by submitting a police report and the IRS ID Theft Affidavit (Form 14039).
- **Contact your state tax organization:** Your state taxes may be affected as well.
- **Document your case:** Download the free ID Theft Help app from ITRC to track your case as you go through the resolution process.
- **File early:** Get your tax refund before thieves do.
- **Call the ITRC:** You can receive no-cost assistance from a victim advisor by calling 888.400.5530.

A REMINDER FROM NCSA AND ITRC

"With the tremendous amount of personal and financial information that is available online, tax season is paradise for cybercriminals. There are many ways that identity thieves can get their hands on your money or your data. Some of them require high-tech skill sets like hacking and writing malicious software. Others are less involved and basically amount to tricking you into complying. Unfortunately, even the most low-tech tax scam can cause lasting and expensive damage," said Michael Kaiser, NCSA's executive director. "Remember that personal information is like money. You must value it and protect it. During intensely busy online timeframes – and throughout the year – it's critical for everyone to learn how to take simple security precautions to protect themselves and their personal information, and to share the responsibility of protecting others online. Practicing good cybersecurity empowers all internet users to reap the benefits of connectivity with greater confidence."

"All of us, from large government agencies down to individual taxpayers, play a significant role in minimizing tax refund fraud," said Eva Velasquez, ITRC president & CEO. "Avoiding scams and fraud attempts is only one part of the prevention equation. It means staying vigilant about where your personal data ends up, monitoring your credit report routinely for signs of suspicious activity, and filing your return as early as possible to beat a thief to it."

RESOURCES TO HELP YOU STAY SAFE THIS TAX SEASON

Here are a few resources that can help you protect your identity and be safer and more secure online this tax season – and year-round:

- STOP. THINK. CONNECT.™ Tips and Advice
- Identity Theft Resource Center
- The Federal Trade Commission's IdentityTheft.gov
- The U.S. Department of Homeland Security's STOP. THINK. CONNECT.™ Identity Theft and Internet Scams Tip Card

FOLLOW US ONLINE AND ON SOCIAL MEDIA

NATIONAL CYBERSECURITY ALLIANCE

STAYSAFEONLINE.ORG

@STAYSAFEONLINE

STAYSAFEONLINE

ITRC IDENTITY THEFT RESOURCE CENTER

IDTHEFTCENTER.ORG

@ITRCSD

ITRCSD

1. https://krebsonsecurity.com/2016/01/ftc-tax-fraud-behind-47-spike-in-id-theft/
2. http://www.accountingtoday.com/news/irs-warns-of-surge-in-phishing-and-malware-schemes-targeting-preparers-and-taxpayers
3. https://www.fool.com/retirement/2016/12/27/3-tax-scams-to-watch-out-for-in-2017.aspx