



STAY SAFE FROM **CYBERCRIME** DURING *TAX TIME*

Everyone's favorite time of year – tax season – is creeping up on the calendar. Tuesday, April 17, may feel eons away, but the filing deadline will be here before you know it. Tax season is primetime for online scams. According to the Federal Trade Commission (FTC), **tax-related identity theft** – when a criminal uses someone else's Social Security number along with other personal data to file an income tax return (and reap any refunds) – is the most common type of identity theft. In fact, a **2017 Identity Fraud Study by Javelin Strategy & Research** revealed that nearly one in three consumers notified that their data has been breached become victims of identity fraud. With the recent Equifax cyberattack still fresh in our minds, more than 145 million Americans' names, addresses, birthdates, Social Security numbers and other sensitive information may be at risk. Cybercriminals are crafty and continuously looking for ways to steal your personal information. The Internal Revenue Service (IRS) indicates that phishing schemes continue to lead its **"dirty dozen" list of 2017 tax scams**. So what is the average American to do? The **National Cyber Security Alliance (NCSA)** and the **Identity Theft Resource Center (ITRC)** have once again joined forces to help consumers keep safe during tax season with tips for identifying cyber scams, actionable online safety steps and what to do if you fall victim to tax identity theft.

SCAMS TARGETING TAXPAYERS

The IRS has seen a surge in cybercriminal swindles directed at consumers. If you protect yourself against these unscrupulous schemes, your identity and tax return will be safer and more secure.

IRS-IMPERSONATION PHONE SCAMS

Callers claiming to be IRS employees – using fake names and phony IRS ID numbers – may ring you and insist that you owe money and 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. The real IRS will not call you and demand immediate payment; in general, it will mail you a bill if you owe money.

MARKED INCREASE IN PHISHING, EMAIL AND MALWARE SCHEMES

Cybercriminals will try to get you to do something so they can steal your personal information. Watch out for unsolicited emails, text messages, 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.



STAY SAFE FROM CYBERCRIME DURING TAX TIME



FRAUDULENT TAX RETURNS

The FTC strongly 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 becomes impossible for a fraudster 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.

TAX PREPARER FRAUD

The overwhelming majority of tax preparers provide honest services, but some unsavory 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.

TAKE ACTION AND STAY CYBER SAFE WITH TAX TIPS

NCSA has some easy-to-use STOP. THINK. CONNECT.™ tips to help protect 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 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 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 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.

FILE YOUR TAX FORMS ON SECURE HTTPS SITES ONLY.

ASK IF YOUR TAX PREPARATION SERVICE HAS CHECKED FOR MALWARE ISSUES.



STAY SAFE FROM CYBERCRIME DURING TAX TIME



WHAT YOU NEED TO KNOW ABOUT TAX IDENTITY THEFT

According to ITRC, the most important step you can do is file early and get your tax refund before thieves do. Follow these steps 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, 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.
- ✓ **Call the ITRC:** You can receive no-cost assistance from a victim advisor by calling 1-888-400-5530.

REMINDERS FROM NCSA AND ITRC

“Cybercriminals love tax season. The enormous amounts of valuable personal and financial information that are shared online during this timeframe make it a haven for hackers. Since most Americans are filing their taxes, deadlines are looming and the cyber thugs are doing everything they can to take full advantage of the opportunity,” said Russ Schrader, the National Cyber Security Alliance’s executive director. “Hackers are masters of social engineering, so when there is increased potential for having 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.”

“Identity thieves continue their tax-time fraud exploits on two fronts: tax identity fraud and IRS imposter scams,” said Eva Velasquez, president & CEO of the Identity Theft Resource Center. “That means every stakeholder needs to increase his/her vigilance in minimizing risk. In our current climate of ubiquitous data breaches, consumers can feel powerless; however, they do play a vital role in the risk equation. By making informed choices when sharing data and identity credentials, filing tax returns as early as possible and verifying they are actually speaking to the IRS, a consumer can thwart identity thieves.”

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 Internal Revenue Service’s **Tax Scams and Consumer Alerts**
- The U.S. Department of Homeland Security’s **STOP. THINK. CONNECT.™ Identity Theft and Internet Scams Tip Card**

STAYSAFEONLINE.ORG



IDTHEFTCENTER.ORG

