McAfee’s Guide to IRS & Tax Season Scams

Top tax scams and tips to stay safe.
Tax Season Is Upon Us

While responsible taxpayers gather their W-2 and 1099 forms in preparation for the tax filing due date, which typically occurs in April, criminals seize this opportunity to scam these people and go after their personal and financial information. These scams come in many shapes and sizes and can be tricky to identify — which is precisely why we’ve created this guide, to help you stop these scams in their tracks and fight back against fraudsters.

In this definitive guide, we will:

- Take a closer look at the sneakiest tax season scams, including the Dirty Dozen
- Provide security best practices for filing taxes
- Discuss how to determine if you’ve been impacted by a tax scam
- Offer insights on what to do if you’re a victim
- Explore identity theft as it impacts consumers at different life stages

Tax season is a time to get your financials in order, not to get scammed by a criminal. We hope this guide will help you garner insights, learn a few best practices, and, ultimately, keep your personal information personal. Now, let’s start by exploring why criminals are big fans of tax season.

Many consumers assume that filing taxes is a make or break situation, a fear that criminals are eager to prey upon.
Why Tax Season?

There’s a lot at stake as a consumer when it comes to filing your taxes. As a result, many people have a deep fear of the Internal Revenue Service (IRS). Much of this fear stems from the IRS\(^1\) being an incredibly powerful entity, combined with the fact that taxes can be quite complicated to file on your own. Contrary to popular belief, filing your taxes is not a matter of being good at math or accounting. Rather, it’s entirely based on knowing what can be deducted and how. The U.S. tax code is also complex in nature, so a statement like “read the statute” doesn’t just mean that — it means “read the statute, and the case law, and develop a sense of how IRS agents are likely to interpret this during an audit.” Most people who aren’t tax professionals simply don’t have the time to delve into these complexities, as they’re busy earning a living in their own careers.

While the intricacy of the tax code is ultimately why we receive tax deductions and credits, its complex nature instills pervasive fears around the government and tax season\(^2\). One common fear? The IRS will come after you if you make a mistake. In reality, if you make an honest mistake on your return, the IRS will usually work with you to address the error without serious repercussions. Taxpayers are also scared of being audited. However, less than 2% of individual returns are audited\(^3\), and most cases involving deficiency don’t require a full-blown audit. Finally, many people fear correspondence from the IRS. Consumers usually think the worst when they see a letter from the IRS, although it’s usually not as bad as they think. Often, it’s just an informational letter, a notice of adjustment, or a notice of deficiency — all of which can be fixed if they are addressed quickly.

Thousands of people fall victim to IRS scams every year as a result of fear tactics used by criminals, losing millions of dollars in the process. The schemes are typically all based in IRS-related trouble, as scammers know consumers’ fear may cause them to not question the legitimacy of the interaction. Criminals also know they can get the most bang for their buck during tax season when it comes to harvesting data. From Social Security numbers to marital status to income amount, tax documents provide hackers with the data they need to pursue identity theft and other attacks.
Deep Dive on the Dirty Dozen

Many of the schemes tax scammers invoke go beyond the basic security threats we hear about daily. Thankfully, the IRS outlines these schemes in an annual list called the Dirty Dozen, highlighting twelve scams consumers should beware of approaching the filing date. Let’s take a look at the most recently available list.

Phishing
Before responding to that email claiming to be from the IRS regarding your tax return, know that phishing is a very common tactic used to bait and hook innocent users into giving up their financial data. Phishing, an attack vector used to trick users into giving up their private information or money, is a common strategy used by criminals as it can be executed in multiple ways. In fact, the IRS reported a steady stream of fake emails, text messages, websites, and social media attempts to steal taxpayers’ personal information last year.

Phone Scams
These scams typically involve a criminal impersonating the IRS via phone and threatening arrest, deportation, or license revocation if the victim doesn’t pay a bogus tax bill. If the victim doesn’t answer the call, the scam artists will typically leave voicemails urging the victim to call back and shell out cash via wire transfer, prepaid debit card, or gift card. Sometimes, scammers will even trick victims into disclosing personal information, which they can then use for identity theft.

Identity Theft
According to the Federal Trade Commission, identity theft occurs when someone uses your Social Security number or other personal information to open new accounts, make purchases, or get a tax refund. While identity theft is a threat that people should be alert to throughout the year, tax season provides criminals with a prime opportunity to file a fraudulent tax return and claim an illegitimate tax refund.

According to the Treasury Inspector General for Tax Administration, phone scams have cost 14,700 victims a total of more than $72 million since October 2013.
More on the Dirty Dozen

**Return Preparer Fraud**
Otherwise known as accountant fraud, this scam involves unscrupulous return preparers tricking clients by perpetrating refund fraud, identity theft, and other malicious scams. According to the IRS, these criminals typically prey on older Americans, low-income taxpayers, and non-English speakers. And while the vast majority of tax professionals provide honest, high-quality service, it’s important for consumers to exercise caution and choose tax preparers wisely.

**Inflated Refund Claims**
If a tax preparer is promising you a hefty tax return that seems too good to be true, it probably is. These scammers might ask clients to sign a blank return, promise a big refund before looking at the client’s records, or charge fees as a percentage of the refund. A falsely reported or inflated refund claim could result in a lost return or penalties and charges from the IRS.

**Falsifying Income to Claim Credits**
Fraudulent return preparers may convince unsuspecting victims to falsely report their income to qualify for tax credits, such as the Earned Income Tax Credit (EITC) — a benefit for working people with low to moderate income. EITC fraud usually takes advantage of fake 1099-MISC forms, a document used to report miscellaneous payments made to non-employee individuals. These forms appear to be issued by a large bank or loan service that the taxpayer has a relationship with, so they feel more inclined to believe it. However, falsifying your income could result in fraudulent tax preparers taking a bigger cut of your return and leaving you to deal with the consequences.

**Falsely Padding Deductions on Returns**
Fraudulent tax preparers could also inflate your deductions or expenses, which could result in someone paying less than they owe or potentially receive a larger refund that the scammer could take a cut of. Fudging these numbers could result in serious consequences, including a $5,000 fine for a frivolous tax return.
Fake Charities
Taxpayers should be on the lookout for con artists disguised as charitable organizations looking to make a profit on donations from unsuspecting contributors. Many schemers use charity names that are similar to familiar or well-known organizations to trick consumers looking to receive a tax deduction for donating.

Excessive Claims for Business Credits
Improperly claiming fuel tax credit could land a taxpayer in trouble with the IRS. This credit is usually limited to off-highway business uses, such as farming, and is consequently not available to more taxpayers. However, an individual or business could make an erroneous claim on their otherwise legitimate return, or an identity thief may claim the credit in a broader scheme. Additionally, taxpayers should avoid the misuse of research credit, an important feature in the tax code to foster research and experimentation by the private sector. Excessive claims for these credits could lead to penalties, interest, and potential criminal incarceration.

Offshore Tax Avoidance
Offshore tax avoidance occurs when an individual attempts to conceal assets or income that is subject to U.S. taxes. These schemes typically involve the creation of structures that make it seem like a foreign entity is the owner of assets and income when the true ownership lies with a U.S. taxpayer.

Frivolous Tax Arguments
A frivolous tax return is one that doesn’t include enough information to verify whether the return is correct or contains information clearly showing that the reported tax was incorrect, all to avoid paying taxes. Criminals who promote frivolous schemes encourage taxpayers to make unreasonable claims, which could result in a penalty of $5,000.

Abusive Tax Shelters
A tax shelter is a financial arrangement made to avoid or minimize taxes, like a student loan. While claiming deductions for student loans is perfectly legal, many individuals and tax scammers use them as fraudulent tax shelters to try and get a deduction they don’t qualify for.
Signs That You May Be a Victim

Recognizing the signs\(^a\) that you may be a victim of an IRS scam could greatly suppress the repercussions. Look out for these indications that you’ve been the victim of tax-related identity theft:

- Your tax return is rejected when you file it. This could occur if a criminal has already filed a fake return using your Social Security number to claim a fraudulent return in your name.

- You receive a letter from the IRS. If the IRS sends you a letter inquiring whether you sent a tax return containing your name and Social Security number, this could indicate that someone has tried filing a return with your information.

- You receive a W-2 or 1099 form from an employer that you haven’t worked for. If you do receive one of these forms from a company you’re unfamiliar with, look up the company’s name online. This will help determine whether the name you know the company by is different from its official name, which is what appears on tax documents.

- You receive a tax refund for a refund you didn’t file for. While this might appear to be a pleasant surprise at first, know that the IRS isn’t just handing out free money and that this could point to tax-related fraud.

- You receive a tax transcript by mail that you never requested. Tax transcripts show most of the line items from your originally filed tax return. However, they don’t show any changes you may have made after you filed the return.

More than 1 million children — or 1.48 percent of minors — were victims of identity theft or fraud in 2017, according to a report from Javelin Strategy & Research.\(^b\)

It’s precisely why this season is so enticing for criminals — a little fear can go a long way.
Protecting Your Identity & Personal Data

It doesn’t matter what stage of life you’re at — your personal identity is incredibly valuable. It is used for everything from applying for federal loans to getting a driver’s license. But because personal identities hold so much value, they are consequently always a prime target for thieves. Here’s how identity theft varies at different stages of life and what you can do to stay vigilant against threats at all ages:

- **18 and under**: Underage consumers usually have a Social Security number and clean or nonexistent credit, which is ideal for identity thieves. This “blank slate” allows a criminal to open new lines of credit before the individual is old enough to catch on. Parents/guardians can help prevent childhood identity theft by keeping the child’s data out of circulation, locking down sensitive documents, freezing the child’s credit, and looking out for red flags like jury summons and collection calls addressed to the child.

- **20s**: Consumers in their 20s are dealing with a flurry of new life experiences. With so much going on, it can be easy for people in their early 20s to lose sight of their identities. That’s why staying educated on common identity theft schemes like phishing emails and social engineering scams designed to compromise user data should be made a top priority.

- **30s-40s**: With kids, mortgages, and car payments, there is even more at stake when it comes to identity theft. Because users in their 30s and 40s have a more established income, they must be vigilant when it comes to monitoring and protecting their online and financial accounts.

- **50s**: Many 50-somethings are becoming empty nesters and have the added responsibility of their children’s college tuition. With more responsibilities, the more risks users incur. To add insult to injury, people in their 50s often have accumulated decades of old bank statements and tax returns, which can prove a gold mine for identity thieves. Those in their 50s should also secure their mail and paper documents to avoid becoming the victim of identity theft.

- **60s and up**: Many consumers begin to think about retiring in their 60s. Additionally, many elderly people spend time in hospitals or nursing homes, where their personal information is passed between many hands regularly. But these are years to be cherished, not to be spent dealing with identity theft. These people should practice proper security hygiene by recognizing phishing attacks and operating safely online.

According to its “Consumer Sentinel Network Data Book 2017,” the FTC fielded reports of identity theft from 61,114 victims between the ages of 20 and 29 in 2017.
Fight Back Against Fraudsters

While recognizing the signs of tax-related fraud helps ease the burdens associated with these schemes, there are multiple steps users can take to prevent becoming a victim of IRS scams in the first place. Here’s what you can do to fight back against tax schemes:

- Tell the Treasury Inspector General for Tax Administration (TIGTA). Report IRS scams online11 or call TIGTA at 1-800-366-4484.
- Forward email messages that claim to be from the IRS to phishing@irs.gov.
- Tell the Federal Trade Commission via the FTC Complaint Assistant on FTC.gov12. Include “IRS scam” in the notes.
- If scammers appear to be impersonating a state tax authority rather than the IRS, contact your state Attorney General’s office.

Staying Secure Now and in the Future

By following the tips in this guide, you can not only be better prepared to ward off IRS scams and tax-related identity theft, but also be acclimated to head off future advanced threats that may emerge out of the digital age. With so much riding on your personal and financial data, being prepared and educated, you can live your online life with ease and connect with confidence.
About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com

Appendix