

## Protecting Yourself from Tax Scams: A Guide for Tax Season

Tax season brings not only the stress of filing returns but also an increased risk of falling victim to scams. As you prepare to file your taxes, understanding common scams and protective measures is essential for safeguarding your personal information and financial security.

### Social Media and Digital Scams:

Tax-related identity theft can occur through various digital channels including email, phone, text messages, and social media. Scammers have become increasingly sophisticated in their approaches. One common tactic involves bogus phone calls or text messages claiming you owe the IRS money, often threatening arrest warrants, law enforcement intervention, deportation, or license revocation. These criminals even program their systems to display IRS phone numbers on your caller ID to appear legitimate.

### Phishing and Smishing Threats:

Email phishing scams represent another significant danger. These fraudulent emails appear to come from the IRS or related programs like the Electronic Federal Tax Payment System (EFTPS), attempting to trick you into revealing personal and financial information through links to fake websites. Some variations include attachments labeled "Tax Account Transcript" that may contain computer viruses or malware, while others falsely claim you're eligible for a tax refund if you follow their instructions.

Remember: The IRS will never initiate contact through email, text message, or social media to request personal or financial information. It's also unusual for the IRS to initiate contact by fax or phone call without prior written notice.

### Protection for Seniors:

Seniors should be particularly vigilant about protecting their personal information. Never provide personal information over the phone, through the mail, or on the internet unless you initiated the contact or are certain of who you're dealing with. Don't carry your Social Security card or documents containing your Social Security Number or ITIN. Only provide your SSN or ITIN to businesses when truly required, not simply because they ask. Additionally, review your Social Security Administration earnings statements annually to catch any fraudulent activity.

### Protections for Businesses and Tax Professionals:

Tax professionals have legal obligations to protect client data. All tax return preparers must

create and implement written information security plans (WISP). Failure to create a WISP may result in a Federal Trade Commission investigation.

Identity Protection PIN Program:

The Identity Protection PIN (IP PIN) is a powerful tool for preventing fraudulent tax returns. This 6-digit number is assigned annually to certain taxpayers and helps prevent others from fraudulently filing a federal income tax return using your SSN or ITIN. Any taxpayer, including spouses and dependents, may request an IP PIN by passing an identity verification process.

You can obtain an IP PIN immediately online at [www.irs.gov/IPPIN](http://www.irs.gov/IPPIN). Once enrolled, you must obtain a new IP PIN each filing season. Alternatively, eligible taxpayers can file Form 15227, Application for an Identity Protection Personal Identification Number, or schedule an appointment at a Taxpayer Assistance Center by calling 844-545-5640.

If you lose or misplace your IP PIN, you can retrieve it by accessing "Get an IP PIN" at [www.irs.gov](http://www.irs.gov) after completing registration and identity verification. If unable to retrieve

This information is provided to you by Arrowhead Tax Service. We make every effort to provide honest and accurate tax information. Please use your discretion before making any decisions based on the information provided, every tax situation is different. If you have any questions, please visit our office or call us at 937-543-5770.