



Tax Season Security: Avoiding Scams and Protecting Your Money

As tax season approaches, so does the heightened risk of falling victim to scams designed to exploit unsuspecting individuals. Tax return scams come in various forms, with scammers using sophisticated tactics to impersonate trusted entities like the IRS, or legitimate tax preparation services. Their ultimate goal is to collect your sensitive personal and financial information, leading to identity theft or monetary loss. Understanding tax return scams and knowing how to protect yourself is crucial. Here are some tips that can help:

- **Be Skeptical of Unsolicited Communications:** Scammers often use emails, phone calls, and text messages to impersonate tax officials or tax preparation services. Be cautious of unexpected communications, and never share personal or financial information without verifying the legitimacy of the request.
- **Verify the Identity of Tax Professionals:** If you're working with a tax professional or using tax preparation software, ensure that they are reputable and trustworthy. Check reviews, ask for credentials, and be wary of services or opportunities that seem too good to be true.
- **Secure Your Personal Information:** Safeguard your Social Security number, financial details, and other sensitive information. Avoid sharing this information through unsecured channels and only provide it to trusted sources.
- **Watch Out for Phishing Scams:** Phishing emails often spike during tax season. Be cautious of emails claiming to be from the IRS or tax software providers. Verify the sender's email address and avoid clicking on links or downloading attachments from unknown sources.
- **Use Secure Wi-Fi and Devices:** When filing your taxes online, make sure you're using a secure and private Wi-Fi connection. Avoid public networks and ensure your devices have updated security software to prevent unauthorized access.
- **REMEMBER:** Legitimate tax authorities and professionals will NEVER contact you by email, phone call, text message, or on social media requesting sensitive personal or financial information. If in doubt, slow down and ask someone you trust for help. Remember to report any suspicious activity to the appropriate authorities.