



The IRS “Dirty Dozen” list, published every year, has a variety of common scams that taxpayers may encounter anytime, but many of these schemes peak during filing season as people prepare their returns or hire someone to help with their taxes. Here are just a few to think about.

- IRS cautions taxpayers on scams involving disasters or charitable causes.
- Tax return preparer fraud makes the list: Choose tax preparers carefully!
- Identity theft remains on IRS’ “Dirty Dozen” list despite progress.
- Be vigilant against phone scams.
- Agency warns taxpayers of pervasive phishing schemes.




Data breach thefts have given thieves millions of identity data points including names, addresses, Social Security Numbers and email addresses. Thieves may try to leverage stolen identities to steal even more data that will allow them to better impersonate taxpayers and file fraudulent tax returns for refunds. And it’s not just the tax payers,


but also the tax preparers, and even payroll departments, that need to be alert.


Scammers will use the regular mail, telephone, social media or email to set


up unsuspecting individuals, businesses, and payroll and tax professionals. Thousands of people have lost millions of dollars, as well as their personal information, to tax scams. So what can we all do?

TAX-TIME SECURITY TAKE-ACTION TIPS


 **When in doubt, throw it out:** Criminals can get access to your personal information by tricking you into downloading attachments or clicking on links in email. If an email seems suspicious, even if you know the source, it’s best to delete it.


 **Lock Down Your Login.** Create long and unique passphrases for all accounts and use multifactor authentication (MFA) wherever possible. MFA will fortify your online accounts by enabling the strongest authentication tools available, and most major email and online tax preparation services have this tool available.

 **Get smart about Wi-Fi hotspots:** Public wireless networks are not secure. If you are filing your taxes online make sure you are doing it on a secure and personal network.

 **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. Remember, the IRS *doesn’t initiate contact* with taxpayers by email, text messages or social media channels to request personal or financial information.

 **Do your research.** Vet your tax preparer before handing over sensitive information. Ask what steps they take to protect your information. Businesses of all sizes are susceptible to cyber thieves, so it is critical you choose a preparer who takes your security seriously.

 **Update your software.** Before filing your taxes at home or work, be sure that all internet-connected devices - including PCs, smartphones and tablets - are running the most current versions of software. Updates include important changes that improve the performance and security of your devices.