

AVOID COMMON SCAMS WHILE FILING YOUR TAX RETURNS

Tax season is well underway and identity thieves are already gearing up to con their way into your bank accounts and tax return. It's a tempting target – more than 130 million taxpayers received refunds totaling nearly \$300 billion during last year's filing season.

Fraudsters will use various scams and schemes to get access to your information, either by stealing it or tricking you into handing it over. Intersections Inc., a leading global provider of consumer and corporate identity risk management services, offers these tips to make sure you have a safe and secure 2010 tax season.

1. Be suspicious of any calls or emails purporting to be from the IRS, no matter what the issue. For example, some scams claim that someone else has already filed tax returns in your name or SSN. The IRS will always write to you first, will rarely call, and will never email you.
2. Never confirm your SSN or bank account details by email or over the phone.
3. If your bank or employer has been taken over lately, be wary of any calls asking that you confirm your tax information or employment status.
4. Guard your mail because it's especially attractive at tax time. Ideally, have your mail delivered to your front door and not to a curbside mailbox. Collect your mail as soon as you can and avoid putting your returns in a curbside mailbox – take them to the post office instead.
5. If you plan to use an online tax preparation service, make sure you stick with a reputable one that has adequate security measures in place. Be wary of emails offering such services because they're often bogus. And be careful when typing in the URL or web address of an online service in case you misspell the name and end up on a fraudulent site that looks like the real one.
6. Make sure your computer is free of malware like computer viruses and spyware that can steal a copy of your SSN or bank account password.
7. Choose your tax preparer carefully and don't be afraid to ask them important security questions, such as how your information is protected in their offices during and after preparation, how long they keep a copy of your tax return, and whether they conduct background checks on their employees.
8. If you owe money to the IRS, try to pay online. If you have to pay by check, spell out the name "Internal Revenue Service" because it's harder to forge than the letters IRS. And don't drop the check in a mailbox – take it to the post office. It's only once a year and is worth the extra effort.
9. Don't email tax information or returns to your accountant. Email is not a secure way to send any document.
10. If you make copies of your return on a photocopying machine, be aware that many machines keep a copy of your pages in short term memory! Using photocopiers in public locations is not recommended.
11. Don't forget to shred any unnecessary documents or copies when tax season is over. Dumpster divers will be on the prowl to get your banking account details and SSNs.

12. If you plan to keep a copy of your tax return on your computer, make sure it is password protected and encrypted to protect it from prying eyes.
13. Finally, check your credit report immediately after tax time and again a few months later to make sure that if your personal information was stolen, it is not being used against you.