

SmartGuard Newsletter

A New Reason It's a Taxing Season

Tax time increases risk of identity theft

W-2s chock full of personal information—including the biggie, social security numbers—arriving in mailboxes everywhere, every day. Loan documents, health benefit payments, and annual investment and banking summaries lying around for all to see as people start working on tax forms. Tax returns being stored and sent through personal computers without updated firewall, anti-virus, and spyware protection.

Tax season—it's a virtual gold mine for identity thieves. With not only your family's social security numbers in hand, but also banking, investment, loan and other important account numbers included on your tax return, criminals can literally hijack your entire life. And once they do, identity thieves go about obtaining credit cards, loans, property, welfare benefits, jobs and even prison sentences in your name.

Good thing there are many ways to safeguard yourself against identity theft during tax time, such as:

Before You File

- If you have an unsecured outside mailbox, be sure to gather your mail every day—leaving papers to collect there can be tempting to would-be thieves. Also, if you do not receive a W-2, bank statement, credit card bill, or other important document in a timely manner, contact your employer or financial provider to get another copy as well as ensure someone hasn't diverted your mail to a new address.
- Keep all paperwork associated with your taxes, such as W-2s, financial statements, receipts, and the like, locked in a safe location in your home. Left loose on a desk, in a brief case, or in your car means your entire financial life is on display for everyone—including unscrupulous people—to see.
- Shred all sensitive personal documents you don't need to file your taxes before recycling them. Identity thieves have been known to rummage through garbage and recycling bins to ferret out names, social security numbers, and other important information.
- Update the firewall, anti-virus, and spyware protection on your computer. Even if you don't plan to file your tax return online this year, there's a good chance you store at least a few pieces of critical personal data on your computer. Keeping your online security systems up-to-date greatly lowers the chance this information will be stolen.

Related News Links

[Newer photocopiers' disk drives present risk of identity theft](#)

[Identity Theft and Tax Time Tips](#)

[Avoiding Identity Theft, Choosing a Tax Preparer and Understanding "Instant Refunds"](#)

[Identity Theft and Your Tax Records](#)

SmartGuard Newsletter

When You File

- Choose your tax preparer carefully. Because the individual or company you pick to prepare and file your tax returns will have access to all your personal financial information, it's important you work with a reputable firm. Be sure to ask how your information will be protected while in the tax preparer's possession, and if they are filing online on your behalf, whether the information will be encrypted. Check your return carefully and never sign blank or partially completed paperwork. Know that only attorneys, CPAs, and IRS agents can represent you in the event of an audit. Check the Better Business Bureau or your state's CPA or bar association to see if your potential preparer has a history of violations or complaints.
- If you are filing online for yourself, make sure you are using an IRS-approved program. Go to www.irs.gov/efile to check the status of your software provider.
- If you are filing a paper return, do not leave it in your mail box at home or at work. Instead, go to the post office to mail your return via an inside mail box or postal agent to ensure it doesn't get intercepted.

An Ounce of Prevention

Tax season presents a great opportunity for identity thieves—don't be one of their victims. Instead, follow the tips above to maintain your good name and ensure that tax time doesn't become an even more taxing time this year.

Tax Time Scams to Avoid

Duplicating your life. Most newer photocopiers are digital, with a hard drive like a computer. Unfortunately, this advanced technology also means your personal information may fall into the wrong hands if the copier's hard drive is stolen. Therefore, it's imperative you make sure the copier you or your tax preparer uses to duplicate your return is protected with an encryption or overwrite mechanism.

Dialing and phishing for dollars. Identity thieves often call or email unsuspecting people while posing as IRS agents. The thieves then ask for personal information such as Social Security and bank account numbers, saying they need it in order to process tax refunds or prevent an audit. Be warned: The IRS never calls or emails asking for bank or Social Security information—so do not reveal these personal details online or over the phone no matter who the person on the other end claims to be. If you receive any questionable calls or emails, you may report them to the IRS Taxpayers Advocates at 877-777-4778 or the FTC at spam@uce.gov.

Making a mint in loan fees. Did you know that tax preparers offering "instant returns" are actually giving you a loan, and making a pretty penny on the loan fees you pay as a result? While not a scam per se, you should know the fees for an instant return carry extremely high interest rates you'll be responsible to pay whether you receive the expected return or not. Better to file online and ask for the IRS to make payment directly to your bank account—you should have your money in approximately ten days.