



## Tax Season Threats

### Can we defend ourselves at every point of vulnerability?

Just in time for tax season, the Government Accountability Office released a new report detailing information security failings at the Internal Revenue Service. This is indeed a chilling proposition – the government agency that collects more of our private data than any other suffers systemic data security lapses, leaving the door open for potential widespread identity theft.

But the problem is bigger than the IRS. Nearly every federal agency investigated so far suffers similar weaknesses. Some lapses, including those at our nuclear research labs, could endanger national security as well as our identities. And the problem is even worse in state and local governments, which offer Internet and paper databases full of our private information, free to the public.

How can government prosecute identity theft at the same time that it enables the crime? In this newsletter, we examine several points of [vulnerability during tax season](#), offer consumers [new ways to help protect their identities](#), and [call on government to improve](#) in this perilous time.

For a complete newsletter archive, visit: [www.identitytheft911.org/newsletters](http://www.identitytheft911.org/newsletters)

To learn about the latest scams on identity theft, visit: [www.identitytheft911.org](http://www.identitytheft911.org)

Comments, questions? Contact us: [media@identitytheft911.com](mailto:media@identitytheft911.com)



# Tax Time is Data Harvest Time

## The five points of vulnerability during tax season

The e-mail's subject line reads: "*Stimulus Payment form it's ready for you to submit.*" The e-mail, adorned with the Internal Revenue Service's abstract-yet-intimidating bald eagle symbol, promises a federal stimulus payment to those who follow a provided link. From there, simply enter a bank account and Social Security number, and you're on your way to receiving your cut of almost a trillion dollars in aid.

Most readers know exactly what this is: a phishing scam. Every year the graphics of the e-mail grow a little more sophisticated, faulty grammar is corrected, the message updated. Last year, phishing e-mails promised simple tax refunds. This year, with all the talk of huge federal spending to boost the economy, most mention the word "stimulus."

And every year many people actually fall for it.

"This is largely an education issue," Sam Masiello, director of threat management at MX Logic, a spam-filtering software company in Englewood, Colorado, recently told *Secure Computing* magazine. "End-users need to be alerted to the fact that the IRS will never communicate via e-mail. The IRS does not know, nor does it care to know, your e-mail address. Getting word out is key."

Last year the IRS named phishing schemes the most dangerous and widespread type of scam affecting taxpayers. But there are many more. From an identity thief's perspective, tax season is "Go Time."

While most consumers see the period between New Year's and the April 15th filing deadline as a dreadful annoyance, criminals see it as a data bonanza. It's the only time of year when hundreds of millions of people take their most personal information, write it down, and mail it. This massive flow of sensitive data presents identity thieves with opportunity at every step.

From the files on our home computers to the tax accountant's office to the mail room to the IRS to the refund check, each link in the tax chain provides data thieves a door to your most important information, and sometimes your money.

"Typically, identity thieves use a victim's personal and financial data to empty the victim's financial accounts, run up charges on the victim's existing credit cards, apply for new loans, credit cards, services or benefits in the victim's name, file fraudulent tax returns or even commit crimes," the tax agency said in a recent press release. "The IRS urges taxpayers to be extra-vigilant."

But how? Here we present the most common types of scams to watch for at every step of the tax filing process.

### **Vulnerability # 1: Your home computer**

Many people use computer programs to track their finances. While online tax products save your information onto password-protected servers, hard copies of software programs such as TurboTax and TaxCut save all the information onto your computer. Both programs give consumers the option to protect this data using passwords, but this step is not mandatory.

All of which leaves your data vulnerable to multiple lines of attack. Perhaps the simplest way for an identity thief to get your information is to break into your house and steal your computer. A lower-risk route is to hack into your machine. Hackers are likely to become a bigger threat in 2009, according to a recent report by the Identity Theft Resource Center. Without encryption or passwords protecting your tax data, a

stolen or hacked computer is an open door to your identity.

Another threat vector on your computer comes from phishing e-mails. Purporting to come from the IRS, and sometimes well-known tax preparation companies like H&R Block, these e-mails ask taxpayers to click on links to web sites or PDF forms where information is entered in exchange for supposed benefits (a speedy return on your tax refund, etc.). Many of these e-mails also contain hidden malware that secretly loads itself onto your computer to steal your private data. These e-mails are always scams.

"As a general rule, the IRS will not send you unsolicited e-mail and or use e-mail to discuss tax account information with you or request personal or financial information from you," according to a recent agency press release. "Additionally, the agency will never ask you for PIN numbers or security passwords for your credit card, bank or other financial accounts."

Finally, if you share music files using programs like Limewire or Kazaa, you may be giving away access to your tax documents along with your copy of the latest L'il Wayne album. Unless you store your data in a lockbox that's protected by a password, encryption or both, you may be leaving yourself vulnerable every time you go online.

### **Vulnerability # 2: Tax preparation services**

Theresa Barnhart planned to use her tax refund last year to pay off two credit cards and cover part of the cost of a trip to Disney World with her two daughters. Instead she discovered that an employee at an H&R Block store in Toledo had stolen her information and used it to file a duplicate set of tax returns. Using Barnhart's name, the thief got a check from the U.S. Treasury for \$7,063.

The two sets of returns fouled Barnhart's relations with the IRS, which meant she had to spend months clearing her name. The Disney World trip was put off indefinitely.

"I've never heard of anybody getting

that kind of money," Barnhart told a reporter with WTVG, Toledo's ABC affiliate. "I was livid. You think you're protected, but you're not."

In another case in White Plains, New York, an office manager at an H&R Block store used information he stole from tax forms, including names, birthdates and Social Security numbers, to withdraw cash from customers' bank accounts, steal their refund checks and charge thousands of dollars on credit cards fraudulently obtained in the victims' taxpayers' names.

The scam was "every American's worst financial nightmare," U.S. Attorney James Comey, prosecutor in the case, told *USA Today*.

What's the best advice for taxpayers looking for someone reputable to help them do their taxes? Initially, it helps to ask around for a good accountant. But when you have found that accountant, do some research. The Washington State Attorney General's Office recommends that you find a preparer who "is affiliated with a professional organization that provides or requires its members to pursue continuing education and holds them accountable to a code of ethics."

### **Vulnerability # 3: The Post Office**

Another type of inside job involves postal workers. Thankfully, this does not appear to be a common occurrence. But when it does happen, it can be surprisingly difficult to detect.

In one case in Orange County, California, an identity theft ring paid postal employees to steal taxpayer information and IRS checks out of the mail stream. The ringleader, named Ky Vu, used the stolen information to open credit card accounts in victims' names, and used stolen identities to cash diverted tax refund checks.

Even though the theft ring involved dozens of people who together stole over \$1 million, it took postal inspectors four years to find the perpetrators and shut the ring down, according to a Department of Justice press release.

#### **Vulnerability # 4: The Internal Revenue Service**

Bad news: The IRS doesn't yet have firm control over its data security. That's the warning from the Government Accountability Office, which recently completed a report detailing the IRS's continued efforts in improving its sprawling IT system.

"Despite IRS's progress, information security control weaknesses continue to jeopardize the confidentiality, integrity, and availability of financial and sensitive taxpayer information," the GAO wrote in its report, released in January.

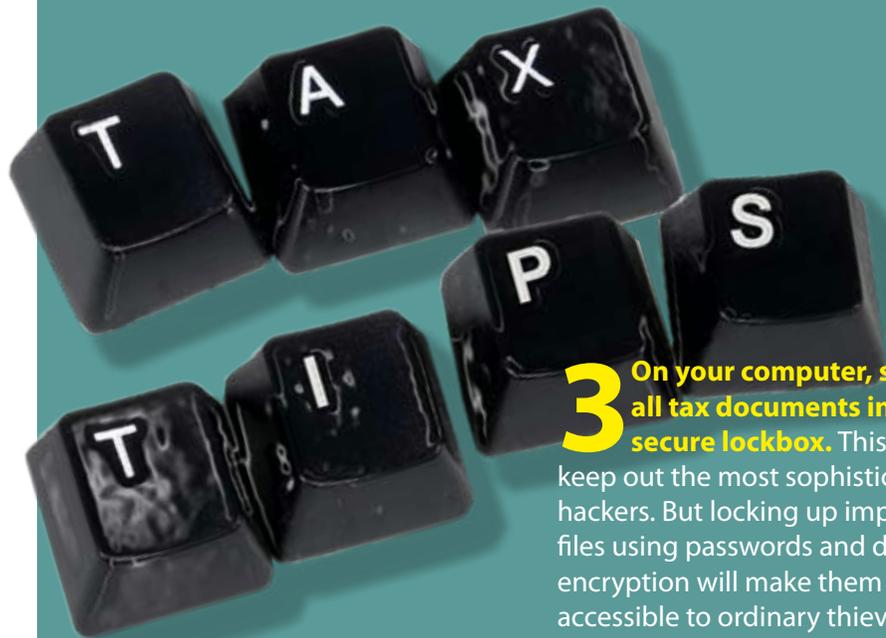
Specifically, this Treasury Department bureau has not completely restricted employee access to tax records, nor has it ensured that only employees with special access obtain important passwords. The agency regularly sends unencrypted data across its internal computer network. It does not monitor changes on its central mainframe to detect unauthorized diversion of data, which could lead to a huge data breach.

#### **Vulnerability # 5: Identity Theft is a threat year-round**

Sometimes tax-related scams are just as random as every other form of identity theft. Michael Tyrone Thomas was arrested in July 2008 for allegedly stealing the private information of 1,132 graduate students at the University of California, Irvine. He filed fake tax returns for 163 of them, according to the campus police chief in an interview with KCAL Los Angeles.

In another case, Kenneth Steve John, aka Dennis Steve John, of Stevenson Ranch, California, was convicted in May 2007 of stealing almost half a million dollars' worth from the IRS by using stolen identities to file fraudulent tax returns on money he won betting at casinos and horse races, according to the *West Branch Beacon*.

While this is a difficult scam to protect yourself against, we do notice one pattern in these cases: Never trust a man with three first names. ■



**It's important to vigilantly guard your identity information all year, but there are a host of vulnerabilities to consider during tax season. Following these tips can help you mitigate the risk of becoming a victim of identity theft.**

**1 Never open an e-mail from the IRS.** And if you accidentally open one, don't click on anything! The reason is simple: the IRS doesn't send e-mails. It's a scam. Likewise, many scammers pose as the IRS online. To contact the real IRS, go to their real website, [www.irs.gov](http://www.irs.gov). It's probably a good idea to be just as vigilant about e-mails from tax preparation services.

**2 Don't send your taxes to an accountant without first determining whether the preparer is reputable.** One way to tell is to determine whether your certified accountant belongs to a national organization that holds its members to a code of ethics.

**3 On your computer, save all tax documents inside a secure lockbox.** This won't keep out the most sophisticated hackers. But locking up important files using passwords and data encryption will make them less accessible to ordinary thieves, whether they enter through the Internet or a broken window.

**4 Pay attention to your snail mail.** Retrieve it from the mailbox every day. If you're going on vacation, even for just a few days, ask a friend to get it for you. Get a locking mailbox or post office box. If bills or documents from your financial institutions don't arrive when you expect them, investigate immediately. Also, if you're expecting a tax return in the mail, make sure you get it. If it seems to be taking a long time, contact the IRS at: 1-800-829-1040.

**5 Don't carry your Social Security card with you, and avoid giving out your Social Security number.** Monitor your bank and credit card accounts at least once a month for fraud. Shred unwanted financial documents and credit cards with a cross-cut shredder—never just throw them in the trash.

If you're worried someone may be using your identity to steal tax returns, check with the Social Security Administration at [www.ssa.gov](http://www.ssa.gov) to see if anyone else is using your Social Security number.



# United States Treasury

## The Weakest Link

### Mapping the Biggest Threats to Our Identities

By Adam Levin

Whether or not you realize it, the Government Accountability Office provided the perfect commencement to the 2009 tax season in January when it published its report on the widespread and persistent threat of identity theft from within the Internal Revenue Service. Of course, "perfect" may not be the first word that came to taxpayers' minds upon hearing that information.

Obviously, I'm entertaining a more expansive meaning of the word "perfect." And the timing of the report is "perfect" precisely because it raises many critical questions during a time when personal data works its way through the virtual and postal channels in a higher volume than any other time of year. But it goes far beyond raising questions solely about government agencies; it challenges us to look at the assumptions we make about just how safe our sensitive personal data is with any monolith to which we're obligated to surrender our data.

Even as the news is saturated with reports on data breaches, let's admit, as consumers we do assume that there still exist sacred cows. Yet with each new breach notification and each new critical data security report, that basic assumption is being proven wrong. Without the GAO's report, we might be inclined to go about our lives in contented oblivion and take for granted that our data is secure when it isn't, in fact, all that secure. If the single largest storehouse of taxpayer information isn't hermetic, as one might

understandably assume, what other stores of our data, be it with a government agency or other organization, are just as vulnerable? Do you really want to know the answer?

If not, you really should want to know.

Though the government's track record isn't a stellar one—a January 2008 GAO report found that 22 of 24 federal agencies failed to implement five important security policies. Among them was the issue of who has access to sensitive data. In many cases, there are too many cooks in the kitchen. In the case of the IRS, nearly everybody working within the organization enjoyed access to tax returns and other sensitive consumer info. But the IRS cannot lay unique claim to putting consumers' identities at risk. Unfortunately.

Many state governments have taken a good, common-sense step toward better protecting citizens' identity information by forbidding private health insurers from issuing insurance cards bearing Social Security numbers. Yet federal government healthcare provider, Medicare, has not removed consumers' Social Security numbers from their cards. A report by the Social Security Administration has unsurprisingly concluded that the cards expose Medicare patients to identity theft. So why hasn't this been resolved? Medicare's reason: it's cost-prohibitive to reprint and reissue the cards. While budgetary concerns are a very real issue to contend with, the tens of millions of

people who currently have Medicare are left unnecessarily exposed to a greater risk of identity theft. A crime, we might add, that is cost-prohibitive for victims.

#### A sobering case

Jeff Fauver knows from the inside how dangerous identity theft can be, especially during tax season. Back when he was the Pentagon's top Internet crimes investigator, he met victims whose lives had been all but commandeered by identity thieves.

That's what Fauver saw when he investigated the case of Chester Charlie Bennington, lead singer of the rap/metal band Linkin Park. A cyber stalker took control of cell phone, PayPal and e-mail accounts belonging to Bennington and his wife, Talinda. The thief used the information to steal money and send disturbing messages that seemed to track the couple's every move.

Fauver's investigation led him to Sandia National Laboratory, a nuclear research facility in New Mexico owned by the Department of Energy and operated by Lockheed Martin. The computers and security systems at Sandia are among the most sophisticated and secure in the world. And yet Devon Townsend, a 27-year-old single mother with limited hacking skills, was able to use those powerful computers and her top security clearance to pry into every aspect of Bennington's life. Thanks to Fauver's

investigation, Townsend was eventually convicted and sentenced to two years in prison for cyber stalking.

This case is especially troubling now, during tax season, because it demonstrates the havoc insiders can wreak. Every spring, hundreds of millions of Americans create documents containing Social Security numbers, bank accounts, phone numbers, etc. They save those documents onto their computers, e-mail them to accountants and send them to the IRS.

At every step, a well-placed insider can hijack that information and use it to carry out all sorts of crimes.

"Government and large corporations are beginning to realize that the real problem is the insider threat," says Fauver, now a cyber security consultant for military contractors and government agencies. "This woman was hacking from inside one of the most secure sites in the world, and she got away with it for a year before she was detected. That shows how serious this is."

### Cracks in the façade

Most businesses and government agencies that handle taxpayers' private data have elaborate and costly systems in place to control physical access to computer files and thwart intrusion by dangerous malware.

The problem, Fauver says, is that in most cases this imposing security façade has many cracks. The most common problem he sees is that companies and government agencies often fail to regularly test their own system once defenses are in place. Most large bureaucracies never create what Fauver calls a "security baseline," which includes a master list of all the people, devices and software allowed to access the system.

Without such a baseline, it's nearly impossible for system administrators to determine which uses are safe and which are not. "That's a very, very weak link," Fauver says.

The other common mistake is that corporations and government agencies,

including those with top-secret missions including defense contractors, fail to test for security gaps after their systems are set up. Is the anti-spyware software actually working? Are only authorized users logging onto secure networks? Bureaucracies that fail to routinely check these areas have no idea.

"They have all the expensive bells and whistles looking at the network traffic," says Fauver. "But they're not looking at the actual logs being generated by those devices. If you don't look at the logs, you don't know what those devices are doing."

### Unintentional negligence

Not all damage is inflicted intentionally. In some cases, Fauver is hired by wealthy individuals to create top-notch security systems for computer networks inside the home. These hard drives may contain client lists, trade secrets, as well as corporate and personal tax documents.

But even the best security system is powerless to protect the network from the homeowner's eldest son, for example, who regularly downloads free games from MySpace loaded with all sorts of nasty malware and password-stealing malicious software.

"If that makes it through the firewall, you could put the entire network at risk," Fauver says. "What if this person is a CPA who works from home? What is he going to tell his clients in two months when he discovers that all of their information has left the network? That could be the end of his business."

So how can government agencies and organizations protect us? Furthermore, how can we protect ourselves?

### The answer

While no security plan is foolproof, Fauver has some great ideas. Most of them focus on demanding responsibility from government, corporations and ourselves. The Government Accountability Office, Congress's

investigative arm, has found persistent computer security failures at nearly every federal agency it has reviewed such as the FBI, the IRS and the Energy Department (including nuclear labs like Sandia). Instead of dealing with these problems on an agency-by-agency basis, we citizens must recognize that the entire federal government has a serious data security problem. And we must push our elected leaders to fix it.

At the corporate level, many of us are about to hand over reams of private data to tax accountants. Some of these companies are themselves sprawling bureaucracies, with their own computer security problems. One way to cope is to ask your accountant how his company plans to keep your data safe. If you use a chain like Jackson Hewitt or H&R Block, the local store worker probably won't know. However, if the company either doesn't know or refuses to tell you, perhaps you should take your business elsewhere.

This gets to the most important point: Ultimately, we are equally responsible for our own data security. As citizens, we must demand that government do a better job of protecting our identities. As consumers, we must vote with our wallets, and only do business with companies dedicated to keeping us safe.

And as individuals, we must protect ourselves. We must buy and use software that secures our computers. We must keep learning about new threats from malicious software and phishing attacks, and we must teach our children and our less tech-savvy relatives and friends how to avoid them. We must never forget our own culpability, and that we do have some say in how we handle our private information.

We must choose wisely. ■