

Protect Yourself from Tax Scams



**CENTER FOR
INTERNET SECURITY®**

William F. Pelgrin, President and CEO

Published March 2013

What is a Tax Scam?

It's tax season and criminals are seizing the opportunity for scams. Don't become the next victim.

Scammers leverage every means at their disposal to separate you from your money, your identity, or anything else of value they can get. They may offer seemingly legitimate "tax services" designed to steal your identity and your tax refund, sometimes with the lure of bigger write-offs or refunds. Scams may include mocked up websites and tax forms that look like they belong to the IRS to trick you into providing your personal information.

According to the IRS, identity theft occurs when someone uses your personal information -- such as your name, Social Security Number (SSN) or other identity information -- without your permission, to commit fraud or other crimes. The Federal Trade Commission estimates that approximately nine million people a year have their identity stolen.

Identity theft often starts outside of the tax administration system when someone's personal information is stolen or lost. Identity thieves may then use a taxpayer's identity to fraudulently file a tax return and claim a refund. In other cases, the identity thief uses the taxpayer's personal information in order to get a job. The legitimate taxpayer may be unaware that anything has happened until they file their return later in the filing season and discover two returns have been filed using the same Social Security number.

Don't let this happen to you. Find out how to protect yourself and your identity during this tax season.

How Can Your Money and Identity be Stolen?

While there are various methods that the fraudsters will utilize to exploit the tax system and people for an easy dollar below are some of the common ones:

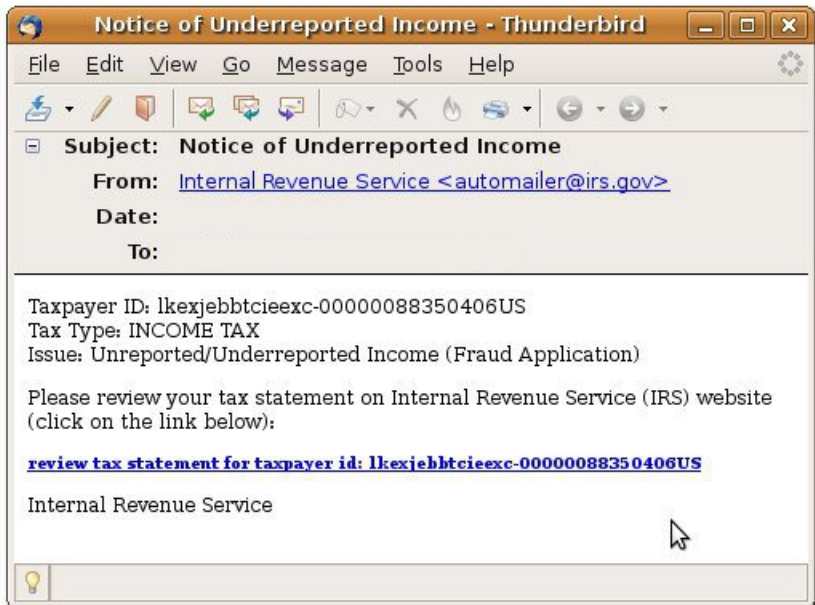


Phishing: In this scam, the fraudsters will send unsolicited emails with links to fake websites, or pop-ups that seek to lure potential victims into providing their personal and financial information. Once armed with the victim's personal information the fraudsters can utilize the victim's identification for fraudulent purposes.

Dumpster Diving: Scammers will often rummage through people's garbage in search of personal information, such as bank account numbers and SSNs.

Pharming: In this scam malware infects the computer and hijacks the web-browser. When you type in legitimate website address you're taken to a fake copy of the site without realizing it. Any information provided on this fake website is then stolen by the fraudster.

Example of a Phishing Scam Email



The email appears to come from the IRS, but note: the IRS does not initiate contact with taxpayers by email or social media tools to request personal or financial information.

The IRS does not send emails stating you are being electronically audited or that you are getting a refund. This includes any type of electronic communication, such as text messages and social media channels.

Example of a Spoofed Website


Please note the multiple categories of detailed personal information being asked for on this page. This is a key indicator that the website is fake.

The IRS does not ask for detailed tax payer personal or financial information on its website.

Sample Page from the Official IRS Website

Get Refund Status x

https://sa2.www4.irs.gov/irfof/lang/en/irfofgetstatus.jsp

 **IRS**.gov

HomeGet Refund StatusRefund Help

Refund Status

Get Refund Status[Obtener Estado de Reembolso](#)

Please enter your Social Security Number, your Filing Status and the refund amount as shown on your tax return.
*See our [Privacy Notice](#) regarding our request for your personal information.

Social Security Number ▶
or IRS Individual Taxpayer Identification Number [shown on your tax return](#).

- -

Filing Status ▶
Please select the Filing Status [shown on your tax return](#).

☐ Single
☐ Married-Filing Joint Return
☐ Married-Filing Separate Return
☐ Head of Household
☐ Qualifying Widow(er)

Refund Amount ▶
You must enter the exact whole dollar amount [shown on your tax return](#). Providing the exact whole dollar amount is essential to receiving the correct response.

\$

Submit

▶ Note: For security reasons, we recommend that you close your browser after you have finished accessing your refund status.

How to Recognize a Tax Scam

According to the IRS, below are the key ways to recognize an email tax scam. The email will:

- request personal and/or financial information (name, SSN, bank or credit card account numbers) or security-related information (e.g. mother's maiden name) either in the email itself or on another site to which a link in the email directs you;
- include exciting offers to get you to respond, such as mentioning a tax refund or offering to pay you to participate in an IRS survey;
- threaten a consequence for not responding to the email, such as additional taxes or blocking access to your funds;
- state that the IRS is holding your refund pending submission of additional personal and financial information;
- has incorrect spelling of the Internal Revenue Service (IRS) or other federal agencies;
- use incorrect grammar or odd phrasing;
- discuss "changes to tax laws" that include a downloadable document (usually in PDF format) that purports to explain the new tax laws. These downloads are populated with malware that, once downloaded, may infect your computer.

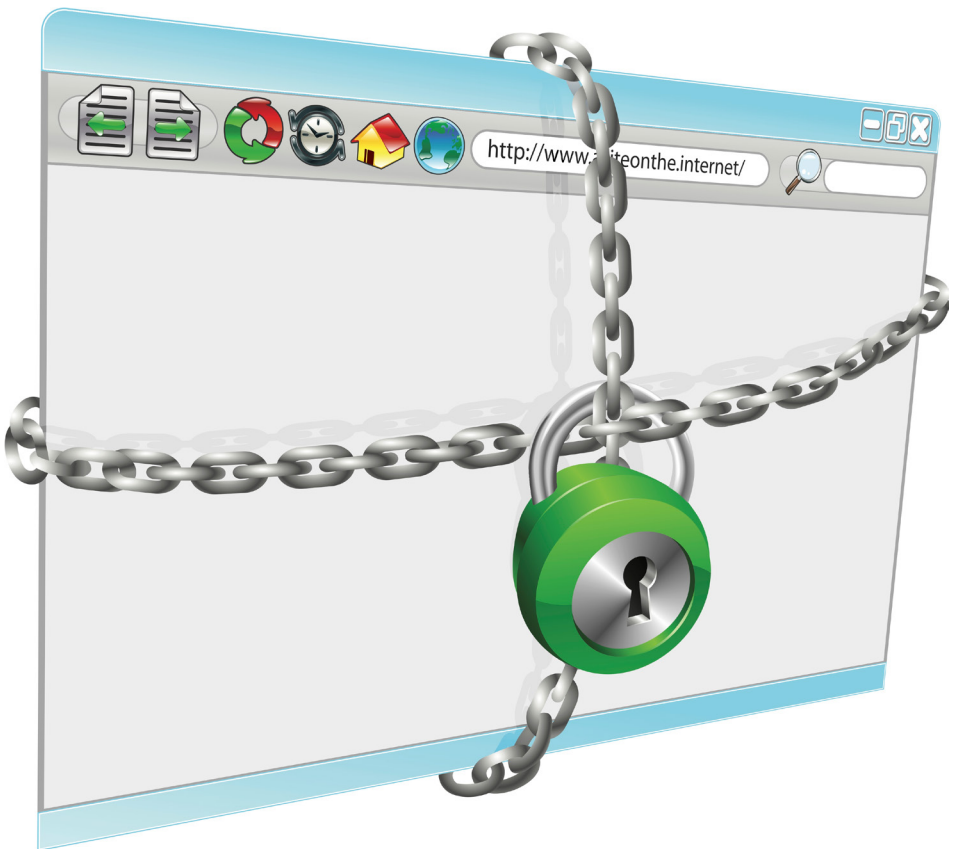
Staying Safe This Tax Season

To help stay safe this tax season, follow these steps:

- 1. Secure your computer.** If your computer does not have proper security controls, it is vulnerable to access by criminals, who may be able to steal information stored on it. Make sure your computer has the latest security updates installed. Check that your anti-virus and anti-spyware software are running properly and are receiving automatic updates from the vendor. If you haven't already done so, install and enable a firewall.
- 2. Carefully select the sites you visit.** Safely searching for tax forms, advice on deductibles, tax preparers, and other similar topics requires caution. Know the site. Know the company. Do not visit a site by clicking on a link sent in an email, found on someone's blog, or on an advertisement. The website you land on may look just like the real site, but it may be a well-crafted fake.
- 3. Don't fall prey to email, web, or social networking scams.** Common scams tout tax rebates, offer great deals on tax preparation or offer a free tax calculator tool. If you did not solicit the information, it's likely a scam. If the email claims to be from the IRS, it's a scam – the IRS will not contact you via email, text messaging or your social network, nor does it advertise on websites. If the email appears to be from your employer, bank, broker, etc. claiming there is an issue with what they reported for you and you need to verify some information, it might be a scam. Contact the entity directly before responding.
- 4. Never send sensitive information in an email.** It may be intercepted and read by criminals.

- 5. Use strong passwords.** Cyber criminals have developed programs that automate the ability to guess your passwords. To protect yourself, passwords must be difficult for others to guess, but at the same time, easy for you to remember. Passwords should have a minimum of nine characters and include upper case (capital letters), lowercase letters, numbers, and symbols. Make sure your work passwords are different from your personal passwords.
- 6. Be wise about wi-fi.** While it may sound relaxing to file your taxes while drinking a triple shot soy mocha-chino at your local café, be wary of transmitting personal information across publicly available wi-fi. These wi-fi hotspots are intended to provide users with a convenient access to the Internet and are not necessarily secure against eavesdropping.
- 7. Don't trust third parties to provide you information on your refund.** To see if you are getting a refund, use the "Where's my Refund" interactive tool located at the IRS website instead of clicking on suspicious links in emails.
- 8. Lock your laptop and mobile device.** Ensure that your laptop and mobile devices are properly locked up. While losing a laptop or a smartphone can be a nuisance, losing them and your identity because you failed to properly lock it up, is even worse!
- 9. Shred documents.** To ensure that your information is properly protected, shred financial statements and other documents that contain your personal information.

- 10. Encrypt your personal data (in transit and at rest).** In addition to locking your computer, ensure that your personal information is properly encrypted both while in transit and also while at rest on your computer. For more information, please read the MS-ISAC newsletter on encryption at: <http://msisac.cisecurity.org/newsletters/2012-09.cfm>
- 11. Check your credit report.** Checking your credit report is one important way to discover whether or not your identity has been compromised. And best of all, you are entitled to one free credit report a year through the three major credit bureaus.



Protect Others and Report Phishing

If you have fallen victim to phishing, immediately change the passwords and PINs on any compromised accounts and any accounts using the same credentials. As a best practice, always remember to have different passwords for different accounts.

You can also file a report with the Federal Trade Commission (FTC) at www.ftc.gov/complaint. In addition follow the steps detailed in the Reporting Identity Theft section of this booklet if you suspect the phishers have stolen your identity.

Even if you did not fall prey, you should still report any phishing attempts to help protect others. Inform the companies that are being impersonated and also report the problem to law enforcement through the National Consumers League Fraud Center at www.fraud.org, the FTC at spam@uce.gov or the Anti-Phishing Working Group at reportphishing@antiphishing.org. In addition you can also forward phishing emails claiming to be the IRS to the IRS mailbox phishing@irs.gov. Once you have forwarded the email, delete the email from your inbox. Please add in the subject line of the email, "Suspicious website."

Remember that phishing is not solely done through the Internet. Fraudsters will utilize any tool they can, including making phone calls or text messages to scam victims. If you receive a suspicious phone call claiming to be from the IRS, ask for a call back number and employee badge number. Then contact the IRS to determine if the caller is a legitimate IRS employee. Likewise, if you are sent a suspicious letter, contact the IRS to determine if the mail is legitimate. In addition if you receive text messages or Short Message Service (SMS) messages claiming to be the IRS, do not respond, open any attachments or click on any links. Forward the text as is to the IRS at 202-552-1226, and if possible also forward the originating number of the suspicious SMS or text message.

Reporting Identity Theft

The following steps detail what should be done if you suspect or know that you have had your identity stolen. While the scammers may have taken your identity to use for tax fraud, they may also use your information to take out loans, open credit cards or establish cellphone plans. If you've been a victim of identity theft, it is essential that you react as quickly as possible to reduce the impacts associated with losing your identity.

Finding and Reporting Identity Theft to the IRS

According to the IRS, your identity may have been stolen if you receive a letter from the IRS or learn from a tax professional that:

1. you filed more than one tax return or someone has already filed using your information;
2. you have a balance due, refund offset or have had collection actions taken against you for a year you did not file;

And/or

3. you receive wages from an employer you have not worked for.

If you receive such a letter from the IRS and you suspect that your identity has been stolen, respond immediately to the name, address, phone number or fax listed on the IRS letter or contact the IRS to determine if the letter is legitimate.

If you become the victim of identity theft outside of the tax system or believe you may be at risk due to a lost/stolen purse or wallet, questionable credit card activity or credit report, you are encouraged to contact the IRS at the Identity Protection Specialized Unit, toll-free at 1-800-908-4490 so the IRS can take steps to further secure your account.

You will need to fill out the IRS identity Theft Affidavit, Form 14039. Please be sure to write legibly and follow the instructions on the form.

Preventing Further Damages from Identity Theft

You should follow the steps below to prevent further malicious activity from occurring:

Place an Initial Fraud Alert

- Contact the three Credit Reporting Agencies.
- After you have confirmed your identity, ask the reporting agencies to establish a credit freeze alert to prevent any additional accounts from opening under your name.
- Close fraudulent accounts.

Equifax
www.equifax.com
1-800-525-6285

Experian
www.experian.com
1-888-397-3742

TransUnion
www.transunion.com
1-800-680-7289

Order your Credit Report

- Placing an initial fraud alert entitles you to free reports from each of the three Credit Reporting Agencies.
- Review these credit reports closely and ensure that your SSN, current address and employer information is accurate.
- Dispute errors with the Credit Reporting Agencies.

Create an Identity Theft Report

Steps to creating an ID Theft report:

- Submit a complaint about the theft to the FTC. When you finish writing all the details, print a copy of the report. It will print as an Identity Theft Affidavit.
- File a police report about the identity theft, and get a copy of the police report or the report number. Bring your FTC Identity Theft Affidavit when you file a police report.
- Attach your FTC Identity Theft Affidavit to your police report to make an Identity Theft Report.

Use the report to:

- get fraudulent information removed from your credit report;
- stop a company from collecting debts that resulted from identity theft, or from selling the debt to another company for collection;
- place an extended fraud alert on your credit report;
- get information from companies about accounts the identity theft opened or misused.

Additional Resources

- Center for Internet Security Multi-State Information Sharing and Analysis Center Tax Tips

Newsletter:

<http://msisac.cisecurity.org/newsletters/2013-03.cfm>

Video:

http://www.youtube.com/watch?v=_WZMUkPj7KM

- IRS Identity Protection Guide
<http://www.irs.gov/uac/Identity-Protection>
- Federal Trade Commission
<http://www.ftc.gov/idtheft>
- Identity Theft Resource Center
<http://www.idtheftcenter.org>
- Identity Theft Assistance Center
<http://www.identitytheftassistance.org>
- Anti-Phishing Working Group
<http://www.antiphishing.org/>

