



March 2023

Cyber Security Awareness Newsletter

Protecting yourself and information from cyber security threats

Tax season is here, and many of us turn to online tax services to file our returns. While online tax services are convenient and easy to use, we must be careful about our cybersecurity when we file our taxes online. Tax refund scams are quickly becoming one of the most common ways thieves steal money and identities. Why is it becoming so popular? Criminals prey on the stress of paying taxes in a timely manner. They know what the deadline is (Tuesday, April 18th) to have tax forms completed and they will ramp up their efforts the closer we get to that date. So, what kind of scams do we see? See below for some of the popular scams of 2022 and how to help defend yourself against these scams.



Pretending to be the IRS

The IRS sends notices and letters for the following reasons:

- You have a balance due.
 - You are due a larger or smaller refund.
 - They have a question about your tax return.
 - They need to verify your identity.
 - They need additional information.
 - They changed your return.
 - They need to notify you of delays in processing your return.
- The #1 information theft venue is e-mail. The IRS does not send e-mail. If you see an e-mail claiming to be from the IRS it is a phishing attempt to get you to click on a link, install software or other malicious action to get your information. The IRS does not use e-mail to communicate, and [they state this on their website](#).



05/18/2017
Reference: I3H583326/16

Claim your Tax Refund Online
Dear Taxpayer,

We identified an error in the calculation of your tax from the last payment, amounting to \$319.95

In order for us to return the excess payment you need to create a e-refund account after which the funds will be credited to your specified bank account.

Please click "Get Started" below to claim your refund:

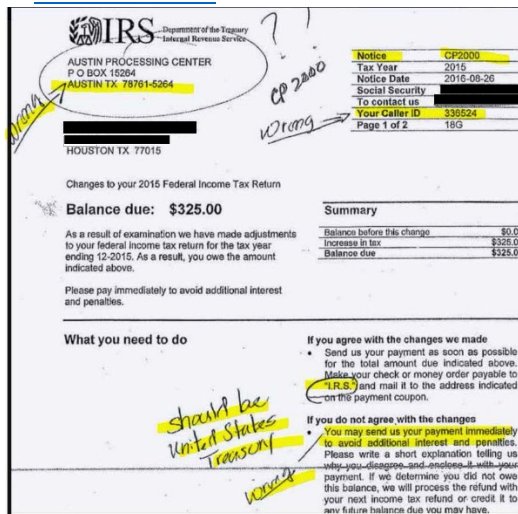
[Get Started](#)

1. Don't click!
2. Simply place the mouse over the link
3. Now see the REAL link!
viruswebsite.net/irns.s/

The IRS doesn't initiate contact with taxpayers by email, text messages or social media channels to request personal or financial information



- A letter from the IRS that gives instructions. If you have any doubts about the legitimacy of a received letter, call: [800-829-1040](tel:800-829-1040).



IRS - Department of the Treasury
Internal Revenue Service

AUSTIN PROCESSING CENTER
P O BOX 15264
AUSTIN TX 78761-5264

HOUSTON TX 77015

Changes to your 2015 Federal Income Tax Return

Balance due: \$325.00

As a result of examination we have made adjustments to your federal income tax return for the tax year ending 12-2015. As a result, you owe the amount indicated above.

Please pay immediately to avoid additional interest and penalties.

What you need to do

If you agree with the changes we made:

- Send us your payment as soon as possible for the total amount due indicated above. Make your check or money order payable to **IRS** and mail it to the address indicated on the payment coupon.

If you do not agree with the changes:

- You may send us your payment immediately to avoid additional interest and penalties. Please write a short explanation telling us why you disagree, and enclose it with your payment. If we determine you did not owe this balance, we will process the refund with your next income tax refund or credit. It to see future balance due you may have.

Summary

Balance before this change	\$0.00
Increase in tax	\$325.00
Balance due	\$325.00

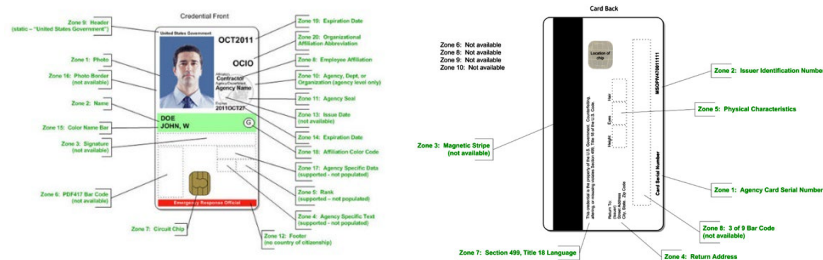
- If the IRS needs to contact a taxpayer by phone, they typically send a notice first, either by mail or through the taxpayer's online account. The notice will provide the IRS employee's name and contact information, along with instructions on how to verify the caller's identity. The IRS will never demand immediate payment over the phone, threaten to involve law enforcement, or ask for credit card or debit card numbers over the phone.



The IRS initiates most contacts through regular mail delivered by the United States Postal Service. However, there are circumstances in which the IRS will come to a home or business. These include when a taxpayer has an overdue tax bill, a delinquent (unfiled) tax return or has not made an employment tax deposit. An IRS employee may also view assets or tour a business

as part of a collection investigation, an audit or an ongoing criminal investigation. So how do you know the person showing up at your door is a scammer or legitimately part of the IRS? There is no foolproof way of identifying a legitimate IRS agent. However, you can ask for identification. Besides regular IDs and business cards, there are two official types of IRS identifications you can request from an agent:

- **HSPD-12 Card:** Also known as a Personal Identity Verification (PIV) card, this is a government identification card with information that you can verify with the IRS. [You can find more information about checking the authenticity of a PIV card here.](#)
- **Pocket Commission:** Another identification card, the pocket commission should include a photo of the agent and information regarding their role within the IRS and specifying which actions they are qualified to carry out.



According to the IRS, you have the right to ask for and view an IRS agent's credentials. If the IRS agent refuses to show you either identification cards, do not give them any personal or tax information. Contact the IRS directly to double-check if there is a legitimate issue or action against you by calling [800-829-1040](tel:800-829-1040).

The Ghost Tax Preparer

If you are hiring a tax professional, work only with a legitimate and reputable Tax Preparer. [You can validate a preparer's credentials with the IRS here.](#)



By law, anyone who is paid to prepare or assist in preparing federal tax returns must have a valid Preparer Tax Identification Number, or PTIN. Any preparer will have a PTIN you can use to verify and check their reputation. Do not hire anyone who promises a high return and charges a

fee based on the return. Avoid a “ghost preparer,” or someone who wants to make a fast buck and does not sign a tax return they prepare.

Ghost tax return preparers may also:

- Require payment in cash only and not provide a receipt.
- Ask for payment in gift cards.
- Invent income to qualify their clients for tax credits.
- Claim fake deductions to boost the size of the refund.
- Direct refunds into their bank account, not the taxpayer's account.
- Never respond to phone calls or voice-messages purporting to be the IRS. The IRS will always contact you by US Mail. Scammers will often use social engineering to create panic in victims, claiming audits, wage garnishment, or other fear inducing terms to trick people into divulging personal information or bank accounts.
- Tax Assistance Program (TAP) scams. Victims receive an offer of assistance in their tax preparation, but after submitting their details, the ghost preparers disappear once they have file the refund, deposit it into their account, or drain the victim’s bank account.



**DON'T
GIVE
SCAMMERS
A GIFT.**

If a caller threatens you unless you give them money via a gift card, they're a scammer. Hang up and report them to the FTC or the police.

FOR MORE INFORMATION, VISIT [TN.GOV/COMMERCE](https://tn.gov/commerce).



Tips for online safety



When filing your taxes online, it's important to be cautious and take steps to protect your personal and financial information. Here are some tips to keep in mind:

- **Use** a trusted tax preparation service: Be sure to use a reputable and trusted tax preparation service to file your taxes online. Research the service beforehand to ensure that they have proper security measures in place to protect your information.
- Use strong passwords: When creating an account or logging in to your tax preparation service, use a strong and unique password that you don't use for any other accounts. Consider using a password manager to generate and store complex passwords securely.
- Enable two-factor authentication: Many tax preparation services offer two-factor authentication, which adds an extra layer of security to your account. Enable this feature if it's available to you.
- Be cautious of phishing scams: Cybercriminals may attempt to trick you into divulging your personal and financial information through phishing scams. Be wary of unsolicited emails or phone calls that request your information, and always verify the legitimacy of the request before providing any information.
- Protect your device: Ensure that your device is up to date with the latest security patches and anti-malware software. Avoid using public Wi-Fi when filing your taxes online, as these networks may be unsecured and vulnerable to attacks.

By following these tips and taking a cautious approach, you can help protect your personal and financial information when filing your taxes online. Remember to stay vigilant and report any suspicious activity to your tax preparation service or the appropriate authorities.